BROCADE
A Broadcom Company

Fabric OS v8.2.3d

Fabric OS v8.2.3d Release Notes

Release Notes

Version 3.0

Table of Contents

Chapter 1: Preface

1.1 Contacting Technical Support for your Brocade® Product

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: ▪ **Case Management** ▪ **Software Downloads** ▪ **Licensing** ▪ **SAN Reports** ▪ **Brocade Support Link** ▪ **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

If you purchased Brocade product support from a Broadcom OEM/solution provider, contact your OEM/solution provider for all your product support needs.

- OEM/solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.

For questions regarding service levels and response times, contact your OEM/solution provider.

To expedite your call, have the following information immediately available:

General Information:

- Technical support contract number, if applicable.
- Switch model.
- Switch operating system version.
- Error numbers and messages received.
- `supportSave` command output and associated files.

  For dual-CP platforms running Fabric OS 6.2 and above, the `supportSave` command gathers information from both CPs and any AP blades installed in the chassis.
- Detailed description of the problem, including the switch or fabric behavior immediately following the problem and any specific questions.
- Description of any troubleshooting steps already performed and the results.
- Serial console and telnet session logs.
- Syslog message logs.

Switch Serial Number.

The switch serial number is provided on the serial number label, examples of which follow:

The serial number label is located as follows:

- Brocade 6520, 6510, 6505, G630, G620, G610 – On the switch ID pull-out tab located on the bottom of the port side of the switch.
- Brocade 7840, 7810 – On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch in a well on the left side underneath (looking from the front).
- Brocade DCX 8510-8 – Bottom right of the port side.
- Brocade DCX 8510-4 – Back, upper left under the power supply.
- Brocade X6-8, X6-4 – Lower portion of the chassis on the nonport side beneath the fan assemblies.

World Wide Name (WWN).

When the Virtual Fabric feature is enabled on a switch, each logical switch has a unique switch WWN. Use the `wwn` command to display the switch WWN.

If you cannot use the `wwn` command because the switch is inoperable, you can get the primary WWN from the same place as the serial number.

License Identifier (License ID).

There is only one license ID associated with a physical switch or director/backbone chassis. This license ID is required as part of the ordering process for new FOS licenses.

Use the `licenseIdShow` command to display the license ID.

1.2 Related Documentation

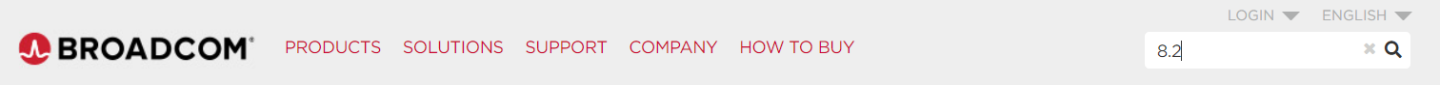
White papers and data sheets are available at www.broadcom.com. Product documentation and release notes for all supported releases is available at www.broadcom.com.

Chapter 2: Locating Product Manuals and Release Notes

This section outlines how to locate and download Brocade product manuals and release notes from myBroadcom. Although the illustrations show Fibre Channel and Fabric OS (FOS), they work for all Brocade products and operating systems.

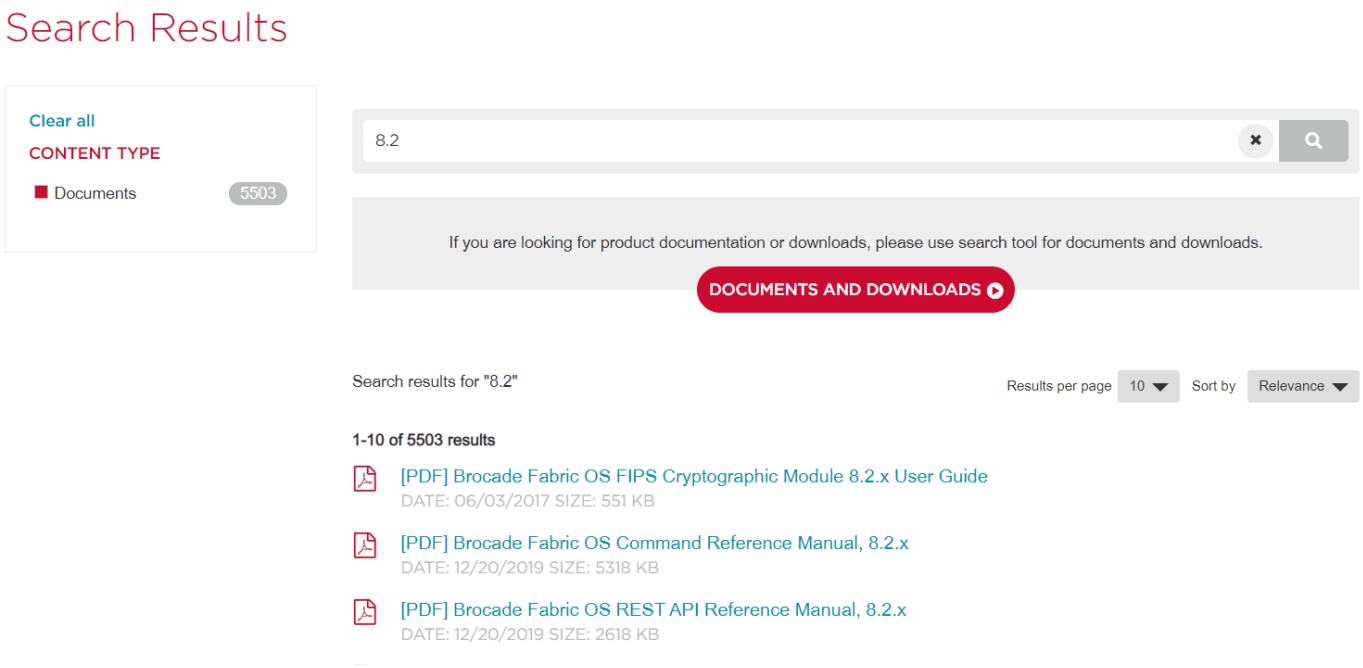
Complete the following steps to locate your product manuals on Broadcom.com.

1. Go to https://www.broadcom.com.
2. Enter the product name or the software version number in the **Search** box.
   For example, the following search is for software and documentation files for software version 8.2.



3. Select the **Documents** check box to list only the documents.

   The list of documents available for the release displays.



2.1 Document Feedback

Quality is our first concern and we have made every effort to ensure the accuracy and completeness of this document. If you find an error or omission or think that a topic needs further development, we want to hear from you. You can provide feedback by sending an email to documentation.PDL@broadcom.com. Provide the publication title, publication number, and as much detail as possible, including the topic heading and page number, as well as your suggestions for improvement.

Chapter 3: Overview

These Release Notes cover Fabric OS v8.2.3d.

Fabric OS v8.2.3d is a patch release based on Fabric OS v8.2.3c/c1.

All Gen 5 hardware platforms and features supported in FOS v8.2.3 are also supported in FOS v8.2.3d including patch releases of 8.2.2 (8.2.2a, 8.2.2b, 8.2.2c, and 8.2.2d). Gen 6 platforms are supported through FOS v8.2.3c. FOS v8.2.3d contains minor enhancements and fixes for the defects listed at the end of this document.

Chapter 4: What's New in FOS v8.2.3d

4.1 Resolution of Important Defects

This release provides the following important defect fixes:

FOS-840370 Firmwareupgrade failed due to time-out from a busy standby CP; HA lost sync after cald panic with a large sized core file and high compact flash usage.

FOS-841163 User can't perform firmware download on the switch from SANNav.

FOS-845216 User may encounter an unexpected sudden system reboot.

FOS-845750 Support for non-disruptive EX port link cost changes.

For a full list of fixes, see Defects.

4.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details, see Software Upgrades and Downgrades.

4.3 Software Features

This release includes the following enhancements.

4.3.1 System Security

FOS v8.2.3d includes the following enhancements and support updates:

- Support single bind for LDAP login

  The following Microsoft LDAP versions are supported:
  - Windows Server 2019, schema 88 -with certificate support
  - Windows Server 2022, schema 88 -with certificate support

Support for previous versions of Microsoft LDAP is deprecated in FOS v8.2.3d.

Chapter 5: What's New in FOS v8.2.3c

5.1 Resolution of Important Defects

This release provides the following important defect fixes:

FOS-839820 Brocade 8510-8 director class switches with a single faulty WWN card, running FOS v8.2.3a or FOS v8.2.3b may encounter a failure reading from the WWN cards.

FOS-826227 Devices in default allaccess zone cannot communicate to each other across LISLs in FICON environment on all platforms.

FOS-836531 Switch panic with maps daemon (MDD) watchdog timeout.

FOS-839346 Path loss experienced after FOS upgrade on Access Gateway.

For a full list of fixes, see Defects.

5.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details, see Software Upgrades and Downgrades.

5.3 Software Features

This release includes the following enhancements.

5.3.1 MAPS

FOS v8.2.3c provides MAPS support for monitoring of the following SmartOptics:

8G DWDM 80 km `[ALL_80Km_8GELWL_SFP]`

16G DWDM 40 km `[ALL_40Km_16GELWL_SFP]`

32G DWDM 40 km `[ALL_40Km_32GELWL_SFP]`

Note: Downgrade from FOS v9.x that support this feature to FOS v8.2.3c (or later) is blocked.

Chapter 6: What's New in FOS 8.2.3b

6.1 Resolution of Important Defects

This release provides the following important defect fixes:

FOS-831875	SNMP application may lose connection to switch momentarily during snmp walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot.
FOS-832434	After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch, with the following error: login: admin "Inconsistency de" -Note: traffic may be impacted too.
FOS-833935	Management application encounters errors after webtool runs out of file descriptor on switches with LDAP configuration.
FOS-834912	SANnav reports error: "Registration for telemetry profile 'xxx' has failed and Switch panic after cald termination.
FOS-836031	Switch panic after FDMI daemon terminated.
FOS-836265	During code upgrade from FOS v8.2.1x to FOS v8.2.3x, FOS cannot completely be brought up due to cald core dumps. User observes the switch hanging if cal.esrs configuration keys are present.

For a full list of fixes, see Defects.

6.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details, see Software Upgrades and Downgrades.

Chapter 7: What's New in FOS 8.2.3a/8.2.3a1

7.1 Resolution of Important Defects

This release provides the following important defect fixes:

- FOS-830052: Port initialization interop issues with a certain SFP, when connecting to a specific 3rd device. This may result in some ports showing errors and some going into no_sync, port_Flt state.
- FOS-831875: SNMP application may lose connection to switch momentarily during SNMP walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot
- FOS-832434: After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch. Error shown as below: login: admin Inconsistency de Note: traffic is impacted too.
- FOS-823756: A third party device is unsuccessful in moving from one switch port to another switch port.
- FOS-828899: DP Panic after upgrading to FOS8.2.1 through FOS8.2.2d while running FICON XRC traffic over XRC Emulation enabled FCIP Tunnel.
- FOS-820640: Flash usage exceeds 90% resulting in a switch panic.
- FOS-827217: Switch panic during tracedump.
- FOS-829779: SANNAV fails to generate switch supportSave on switches running FOS v8.2.2 and above.
- FOS-827821: Device has login issue with certain optic types.

7.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details see Software Upgrades and Downgrades.

7.3 Software Features

FOS 8.2.3a includes the following CLI enhancements.

7.3.1 CLI Enhancements

sysHealth

New command to perform PCIe link test between the Standby CP and the port or core blades in the chassis.

Use this command to run system health related tests.

Synopsis

syshealth --slotpcitest slot_number
syshealth --slotpcitest all
syshealth --help

aaaConfig

New option `-tls_mode` added to specify the mode of the connection with the LDAP Server.

Valid options include the following:

starttls

Initiates LDAP connection with StartTLS. The default port is 389.

ldaps

Initiates LDAPS connection. The default port is 636.

Synopsis

aaaconfig --add | --change server -conf radius | ldap | tacacs+
[-p port] [-d domain] [-t timeout] [-s secret]
[-a chap | pap | peap-mschapv2] [-e -encr_type none | aes256]
[**-tls_mode starttls | ldaps**]

NOTE In a chassis, both CPs must be loaded with FOS v8.2.3a before configuring the LDAPS protocol. Before configuring LDAPS, verify that both CPs are running FOS v8.2.3a; otherwise, the command results in a no-op operation if the standby CP does not support LDAPS.

When LDAP TLS Mode configuration is set to LDAPS in FOS v9.0.1x, it's not recommended to downgrade to FOS v8.2.3a.

If downgrade to FOS v8.2.3a from FOS v9.0.1x is necessary, first configure LDAP TLS Mode to STARTTLS before downgrading to FOS v8.2.3a to avoid potential user login issues.

portCfgLosstov

New options `-dwdmloyncon` and `-dwdmlosyncoff` added to enable or disable the configuration for DWDM lossSync fixed speed port.

Synopsis

portcfglosstov port [-dwdmlosyncon | -dwdmlosyncoff]

Chapter 8: What's New in FOS 8.2.3

8.1 Resolution of Important Defects

This release provides the following important defect fixes:

- FOS-825388: FCIP Tunnel up, but all I/O stops flowing over the tunnel and application times out.
- FOS-823765: Traffic disruption encountered when Encryption block errors occur due to errors, such as, "frames too long".
- FOS-823769: HA state went out of sync after duplicate "zonecreate --peerzone" and cfgadd CLIs.
- FOS-826655: Switch panic during code upgrade in a virtual fabric, if there were with stale LISL leftover from previous switchdisable/switchenable operations.
- FOS-800300: After running diagnostic test on G630, it cannot pass traffic without a reboot first.

Chapter 9: What's New in FOS 8.2.2

9.1 Software Features

The following sections list new, modified, and deprecated software features for this release.

9.1.1 Modified Software Features

This release includes the following enhancements to existing features and supports:

- Support 10Gb/s Ethernet ports in Brocade 7810 base configuration without the Extension Upgrade license.
- Support a user configurable port for SCP and SFTP protocols with the `firmwareDownload` and `supportSave` commands.
- Support a user configurable port attribute for SCP and SFTP protocols with the `brocade-operation-supportsave` REST API module.
- Support REST API GET operation without a session authorization key. HTTP GET operations can be completed with a single request using a Basic Authentication header.

9.1.2 Deprecated Software Features

This release includes the following deprecation of existing features and supports:

- The IPSec feature on Management Ethernet Interface is deprecated. Hence, the `ipsecconfig` CLI command is deprecated.
- The `switchUptime` CLI command is deprecated.

Chapter 10: What's New in FOS 8.2.1

10.1 Hardware

The following sections list new hardware introduced with this release and hardware that is no longer supported with this release.

10.1.1 New Devices

Product Name	Device Name
Brocade 7810	Gen 6 (32Gb/s) Distance Extension Switch

10.1.2 New Blades

None.

10.1.3 New Optical Transceivers

FOS 8.2.1 supports the following new optical transceiver on the noted devices:

- 32Gb/s Fibre Channel 25 KM ELWL SFP (customer P/N XBR-000278) on the Brocade G620, G630, FC32-48, and SX6 blade.

10.1.4 Deprecated Hardware

None.

10.2 Software Features

The following sections list new, modified, and deprecated software features for this release.

10.2.1 New Software Features

The following software features are new in this release:

- Counterfeit License Protection
- REST API with New RESTCONF Modules
- Management Interface Rate Limiting

10.2.1.1 Counterfeit License Protection

FOS 8.2.1 introduces counterfeit license protection (CLP) on the Brocade 6505, 6510, G610, G620, and 7810 to prevent misuse of the **`licenseAdd`** command. CLP performs the following actions based on the number of times that the **`licenseAdd`** command is invoked:

- RASLOG WARNING message when 25 invalid **`licenseAdd`** operations are detected within a 24-hour period.
- RASLOG CRITICAL message when 40 invalid **`licenseAdd`** operations are detected within a 24-hour period.
- Shuts down a switch when 50 invalid **`licenseAdd`** operations are detected within a 24-hour period.

A switch that is shut down due to CLP detection will no longer be able to boot to a functional state. Customers may request a replacement unit from their support provider.

10.2.1.2 REST API with New RESTCONF Modules

FOS 8.2.1 expands REST API support from that supported in FOS 8.2.0a with the following new features and corresponding RESTCONF modules:

- Physical chassis, FRU, and optical transceiver: brocade-chassis, brocade-fru, and brocade-media
- Switch configuration: brocade-fibrechannel-configuration
- SupportSave: brocade-operation-supportsave and brocade-operation-showstatus
- Trunking: brocade-fibrechannel-trunk
- RASLOG and syslog configuration: brocade-logging
- System security: brocade-security
- System time zone and time server: brocade-time
- Monitoring and Alerting Policy Suite (MAPS): brocade-maps

FOS 8.2.1 enhances the following existing RESTCONF modules:

- brocade-fibrechannel
- brocade-fibrechannel-switch
- brocade-access-gateway

For a detailed description of the new modules and attributes, refer to the *Brocade Fabric OS REST API Reference Manual* for FOS 8.2.1.

10.2.1.3 Management Interface Rate Limiting

FOS 8.2.1 implements hardware-based ingress rate limiting on the management interface of X6 directors to prevent denial of service (DOS) attacks through the Ethernet management interface. When this feature is enabled, hardware performs ingress rate limiting when a DOS attack on the Eth0 or Eth3 management interface is detected. Normal management application traffic from Web Tools and SNMP is not affected when there is no DOS attack. These applications may appear sluggish when a DOS attack is detected.

10.2.2 Modified Software Features

The following software features have been enhanced in this release:

- MAPS (Monitoring and Alerting Policy Suite)
- Access Gateway
- Fabric Services
- System Security
- configure Command Enhancements

- Extension
- Power supply microcontroller firmware utility
- Miscellaneous

10.2.2.1 MAPS Enhancements

10.2.2.1.1 UCS/FI Login Imbalance Monitoring

FOS 8.2.1 adds MAPS monitoring of Cisco UCS Fabric Interconnect (FI) connections to Brocade switches in NPV mode. MAPS monitors the distribution of UCS servers over the uplinks between FI and Brocade switches to remain balanced over time. When MAPS detects an imbalance, it alerts the SAN administrator of the condition or triggers an automatic rebalance action.

10.2.2.1.2 Miscellaneous

10.2.2.1.2.1 Default Rule Change

FOS 8.2.1 replaces the default rule names in FOS 8.2.0x detailed in the following table with the new default rule names:

FOS 8.2.0x Rule Names	FOS 8.2.1 Rule Names
defALL_DPIP_EXTN_FLOW_C	defALL_DPIP_EXTN_FLOW_P_90
defALL_DPIP_EXTN_FLOW_M	defALL_DPIP_EXTN_FLOW_P_80
defALL_DPIP_EXTN_FLOW_A	defALL_DPIP_EXTN_FLOW_P_65
defALL_DPIP_EXTN_FLOW_MAX	defALL_DPIP_EXTN_FLOW_P_TOTAL

NOTE The default rules will be automatically converted to the new rule names during firmware upgrade from FOS 8.2.0x to FOS 8.2.1 or later. However, user-defined rules of the IP_EXTN_FLOW monitoring system must be changed manually to follow the new rule name format.

10.2.2.1.2.2 Alert Severity Change

FOS 8.2.1 changes the alert severity from ERROR to CRITICAL for the following default rule:

defALL_E_PORTSC3TXTO_20 ALL_E_PORTS(C3TXTO/MIN>20) RASLOG

FOS 8.2.1 changes the alert severity from WARNING to ERROR for the following default rule:

defALL_FANFAN_STATE_FAULTY ALL_FANS(FAN_STATE/NONE==FAULTY) RASLOG

10.2.2.2 Access Gateway Enhancements

10.2.2.2.1 Slow-Drain Device Quarantine on AG

FOS 7.4 and later support Slow-Drain Device Quarantine (SDDQ) to mitigate congestion due to slow-drain devices connected to switches in native mode. FOS 8.2.1 enhances SDDQ support on AG to be able to quarantine slow-drain devices connected to Access Gateway.

10.2.2.2.2 Port NPIV Configuration

FOS 8.2.1 adds support of the **`portCfgNpivPort`** command for a switch in AG mode. With this support, administrators can enable or disable NPIV mode for a port when a switch is in Access Gateway mode.

10.2.2.3 Fabric Services Enhancements

10.2.2.3.1 GZS and GAZS Commands

FOS 8.2.1 adds support of the Get Zone Set (GZS) and Get Active Zone Set (GAZS) commands under FC-GS-8 for zone servers. GZS queries for Zone Set Database, whereas GAZS queries for Active Zone Set (or Effective Configuration Set).

10.2.2.3.2 Impaired Port Enhancements

FOS 8.2.1 enhances the impaired port feature introduced in FOS 8.2.0. With FOS 8.2.0, an impaired port can be used as a principal link, which is used in fabric-related events, even though there are parallel nonimpaired links available. With FOS 8.2.1, when a principal link is impaired and parallel links exist, an alternate link will be selected as the principal link.

10.2.2.4 System Security Enhancements

10.2.2.4.1 Minimum Password Difference

FOS 8.2.1 adds the new **`-minDiff`** `to` **`passwdcfg`** CLI command to enable SAN administrators to configure the password policy to require the minimum number of characters that must be different between a current password and a new password.

10.2.2.4.2 Session Logout Message

FOS 8.2.1 displays a logout message for SSH or Telnet session logout, exit, or timeout on the standard session terminal window.

10.2.2.4.3 rootAccess Command Change

FOS 8.2.1 adds the **`-force`** option to the **`rootAccess`** command to bypass the interactive prompt of the command execution.

10.2.2.4.4 HTTPS KeepAlive

FOS 8.2.1 adds support of HTTP server connection KeepAlive. The server KeepAlive is supported only with secure HTTPS connections to switches. The KeepAlive support may be enabled with the command `mgmtapp --enable keepalive` in FOS 8.2.1 or later.

10.2.2.5 configure Command Enhancements

FOS 8.2.1 introduces options to the **`configure`** CLI command to allow a number of switch configuration parameters to be set without going through the interactive CLI menu. For details, refer to the *Brocade Fabric OS Command Reference Manual* for FOS 8.2.1.

10.2.2.6 Extension Enhancements

FOS 8.2.1 supports dynamic LAG (LACP) on Gigabit Ethernet LAN ports on extension platforms.

10.2.2.7 Power Supply Microcontroller Firmware Utility

Some power supply models for Brocade Gen 6 platforms support field upgrade of the firmware image used by their microcontrollers. FOS 8.2.1 introduces the `psutil` CLI command for field upgrade of the power supply microcontroller firmware. The power supply firmware is packaged as part of FOS 8.2.1 and later. Administrators can use the **`psutil`** command to check the power supply firmware version and when necessary upgrade to a later version.

10.2.2.8 Miscellaneous Enhancements

FOS 8.2.1 includes the following miscellaneous enhancements:

10.2.2.8.1 chassisName Command

FOS 8.2.1 enhances the **`chassisName`** command to increase the name length from 15 characters to 31 characters on the DCX 8510 and X6 directors.

10.2.2.8.2 ISL R_RDY in Base Switch

FOS 8.2.1 supports the **`portcfgislmode`** command to configure ISL R_RDY mode on the ISLs in a base switch, that is, the XISLs. With this enhancement, devices that support R_RDY mode can also be used on XISLs.

10.2.2.8.3 sfpShow -link Enhancement

FOS 8.2.1 displays the alert thresholds for peer port optics through the **`sfpShow -link`** option. The alert thresholds are displayed for voltage, temperature, Tx Bias, Tx Power, and Rx Power metrics. The alert thresholds are displayed for peer port optics only.

10.3 CLI Command Changes

The following sections list new, modified, and deprecated commands for this release.

10.3.1 New Commands

The following commands are new in this release:

- bladePortMap
- deviceLogin
- factoryFanShow
- psUtil

10.3.2 Modified Commands

Refer to the Modified Commands section of the *Brocade Fabric OS Command Reference Manual* for Fabric OS 8.2.1.

10.3.3 Deprecated Commands

The *Brocade Fabric OS Command Reference Manual* documents all FOS commands that are officially supported. Any commands not listed in the command reference for a specific release are not supported and may be subject to removal without notification. Refer to the Deprecated Commands section in the *Brocade Fabric OS Command Reference Manual* for Fabric OS 8.2.1.

10.4 Supported Standards and RFCs

This software conforms to the Fibre Channel standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. For a list of FC standards conformance, visit the following Broadcom SAN Standards website:

https://www.broadcom.com/support/fibre-channel-networking/san-standards/

Chapter 11: Software License Support

11.1 Optionally Licensed Software

Fabric OS 8.2 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled using license keys.

Optionally licensed features include:

Brocade Ports on Demand – This license allows customers to instantly scale the fabric by provisioning additional SFP ports via license key upgrade. (Applies to select switch models.)

Brocade Q-Flex Ports on Demand – This license allows customers to further scale the fabric and increase flexibility by provisioning additional 4x32G QSFP ports via license key upgrade. (Applies to the Brocade G620 only.)

Brocade Extended Fabrics – This license provides greater than 10 km of switched fabric connectivity at full bandwidth over long distances (depending on the platform, this can be up to 3000 km).

Brocade ISL Trunking – This license provides the ability to aggregate multiple physical links into one logical link for enhanced network performance and fault tolerance. It also includes Access Gateway ISL Trunking on those products that support Access Gateway deployment.

Brocade Fabric Vision – This license enables support for MAPS (Monitoring and Alerting Policy Suite), Flow Vision, and ClearLink (D_Port) when connecting to non-Brocade devices. MAPS enables rules-based monitoring and alerting capabilities, and it provides comprehensive dashboards to quickly troubleshoot problems in Brocade SAN environments. Flow Vision enables host-to-LUN flow monitoring, application flow mirroring for nondisruptive capture and deeper analysis, and a test traffic flow generation function for SAN infrastructure validation. Support for D_Port to non-Brocade devices allows extensive diagnostic testing of links to devices other than Brocade switches and adapters.

NOTE On Brocade G620, G630, Brocade X6-8, and Brocade X6-4 platforms, this license enables the use of IO Insight capability. The license itself is identified as “Fabric Vision and IO Insight” on these platforms.

FICON Management Server – Also known as CUP (Control Unit Port), this license enables host control of switches in mainframe environments.

Integrated Routing – This license allows any Fibre Channel port in a DCX 8510-8, DCX 8510-4, Brocade 6510, Brocade 6520, Brocade 7840, or Brocade G620 to be configured as an EX_Port supporting Fibre Channel Routing (FCR). This eliminates the need to add an FR4-18i blade or use a Brocade 7500 for FCR purposes, and it also provides either quadruple or octuple the bandwidth for each FCR connection (when connected to another 16Gb/s- or 32Gb/s-capable port).

Integrated Routing Ports on Demand – This license allows any Fibre Channel port in a Brocade 7810, G630, X6-8, or X6-4 to be configured as an EX_Port supporting Fibre Channel Routing. The maximum number of EX_Ports supported per platform is provided in the license. This eliminates the need to add an FR4-18i blade or use a Brocade 7500 for FCR purposes, and it also provides octuple the bandwidth for each FCR connection (when connected to another 32Gb/s-capable port).

Advanced Extension – This license enables two advanced extension features: FCIP Trunking and Adaptive Rate Limiting. The FCIP Trunking feature allows multiple IP source and destination address pairs (defined as FCIP circuits) via multiple 1GbE or 10GbE interfaces to provide a high-bandwidth FCIP tunnel and failover resiliency. In addition, each FCIP circuit supports four QoS classes (Class-F, High, Medium, and Low Priority), each as a TCP connection. The Adaptive Rate Limiting feature provides a minimum bandwidth guarantee for each tunnel with full utilization of the available network bandwidth without impacting throughput performance under a high-traffic load. This license is available on the DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis. The upgrade license on Brocade 7810 includes this license to enable 10GbE ports.

10GbE FCIP/10G Fibre Channel – This license enables the two 10GbE ports on the FX8-24 and/or the 10G FC capability on FC16-xx blade ports supported on DCX 8510 platforms except for the FC16-64 blade. On the Brocade 6510 and Brocade 6520, this license enables 10G FC ports. The upgrade license on Brocade 7810 includes this license to enable six 10GbE ports. This license is not applicable to the Brocade 7840, Brocade G620, or Brocade X6 platforms.

On the FX8-24:

With this license installed and assigned to a slot with an FX8-24 blade, two additional operating modes (in addition to 10x1GbE ports mode) can be selected:

10x1GbE ports and 1x10GbE ports
or

2x10GbE ports

On the FC16-xx:

Enables 10G FC capability on an FC16-xx blade in a slot that has this license.

On the Brocade 6510 and Brocade 6520:

Enables 10G FC capability on Brocade 6510 and Brocade 6520 switches.

This license is available on the DCX 8510-8 and DCX 8510-4 on an individual slot basis.

Advanced FICON Acceleration – This licensed feature uses specialized data management techniques and automated intelligence to accelerate FICON tape read and write and IBM Global Mirror data replication operations over distance, while maintaining the integrity of command and acknowledgement sequences. This license is available on the Brocade 7840 and the Brocade DCX 8510-8 and DCX 8510-4 for the FX8-24 on an individual slot basis.

ICL POD License – This license activates ICL ports on DCX 8510 or X6 platform core blades. An ICL license must be installed on the director platforms at both ends of the ICL connection.

On the Brocade DCX 8510-8 and X6-8:

The first ICL POD license enables 16 (half of the total) UltraScale ICL QSFP ports on the DCX 8510-8 or X6-8 Directors, enabling 8 ICL ports on each core blade. These are QSFP port numbers 0, 1, 2, 3, 4, 5, 6, and 7 on the DCX 8510-8; while on the X6-8, the QSFP port numbers are 0, 1, 2, 3, 8, 9, 10, and 11. The second ICL POD license enables the remaining 16 UltraScale ICL QSFP ports on the directors. These are QSFP port numbers 8, 9, 10, 11, 12, 13, 14, and 15 on each core blade of the DCX 8510-8; while on the X6-8, these are QSFP port numbers 4, 5, 6, 7, 12, 13, 14, and 15 on each core blade.

Note that the trunk boundaries are different between CR32-8 core blades on the X6-8 and CR16-8 core blades on the DCX 8510-8.

On the Brocade DCX 8510-4 and X6-4:

ICL POD licenses are different between X6-4 and DCX 8510-4 Directors. On the X6-4, the first ICL POD license enables 8 (half of the total) UltraScale ICL QSFP ports on the director, enabling 4 ICL ports on each core blade, which are QSFP port numbers 0, 1, 4, and 5. The second ICL POD license on the X6-4 enables the remaining 8 UltraScale ICL QSFP ports on the director, which are QSFP port numbers 2, 3, 6, and 7 on each core blade. On the DCX 8510-4, a single ICL POD license enables all 16 UltraScale ICL QSFP ports on the director.

Enterprise ICL (EICL) License – The EICL license is required on a Brocade DCX 8510 chassis when that chassis is connected to four or more Brocade DCX 8510 chassis via ICLs. This license is not applicable to X6 Directors.

This license requirement does not depend upon the total number of DCX 8510 chassis that exist in a fabric, but only on the number of other chassis connected to a DCX 8510 via ICLs.

NOTE The EICL license supports a maximum of nine (9) DCX 8510 chassis connected in a full-mesh topology or up to twelve (12) DCX 8510 chassis connected in a core-edge topology. Refer to the *Brocade SAN Scalability Guidelines* document for additional information.

WAN Rate Upgrade 1 License – The WAN Rate Upgrade 1 license provides additional WAN throughput up to 10Gb/s on a Brocade 7840. The base configuration for a Brocade 7840 without this license provides WAN throughput up to 5Gb/s.

WAN Rate Upgrade 2 License – The WAN Rate Upgrade 2 license provides unlimited WAN throughput (up to the hardware limit) on a Brocade 7840. WAN Rate Upgrade 2 licenses also enable the use of two 40GbE ports on a Brocade 7840. The 40GbE ports cannot be configured without the WAN Rate Upgrade 2 license. A WAN Rate Upgrade 1 license must be installed on a Brocade 7840 before a WAN Rate Upgrade 2 license is installed. A WAN Rate Upgrade 1 license cannot be removed before the WAN Rate Upgrade 2 license has been removed.

NOTE The WAN Rate Upgrade 1 and WAN Rate Upgrade 2 licenses apply only to Brocade 7840 platforms. They control the aggregate bandwidth for all tunnels on that Brocade 7840. The entire capacity controlled by the licenses can be assigned to a single tunnel, or a portion of the capacity can be assigned to multiple tunnels. The total bandwidth aggregated for all tunnels should not exceed the limits established by the licenses.

Extension Upgrade License – The Extension Upgrade license is available on the Brocade 7810, enabling additional ports, capacity, and features that provide the following: 12 32Gb/s FC ports, 6 10Gb/s Ethernet ports, 4 tunnels, 6 circuits per tunnel, 2.5Gb/s WAN throughput, Fabric Vision, Extension Trunking, Brocade ISL Trunking, Integrated Routing Ports on Demand, and Brocade Extended Fabrics. This license is shown as a combination of existing FOS licenses that enable the above capabilities and features.

NOTE FOS v8.2.2 and later supports 6 10Gb/s Ethernet ports in base configuration of Brocade 7810. 10Gb/s Ethernet ports can be enabled without the Extension Upgrade license.

11.2 Temporary License Support

The following licenses are available in Fabric OS 8.2.2 as either universal temporary or regular temporary licenses:

- Fabric (E_Port)
- Extended Fabric
- Trunking
- High Performance Extension
- Advanced Performance Monitoring
- Fabric Watch
- Integrated Routing
- Integrated Routing Ports on Demand
- Advanced Extension
- Advanced FICON Acceleration
- 10GbE FCIP/10GFibre Channel
- FICON Management Server (CUP)
- Enterprise ICL
- Fabric Vision
- WAN Rate Upgrade 1
- WAN Rate Upgrade 2
- Extension Upgrade

NOTE Temporary licenses for features available on a per-slot basis enable the feature for any and all slots in the chassis.

Temporary and universal temporary licenses have durations and expiration dates established in the licenses themselves. FOS will accept up to two temporary licenses and a single universal license on a unit. Universal temporary license keys can be installed only once on a particular switch, but they can be applied to as many switches as desired. Temporary use duration (the length of time for which the feature will be enabled on a switch) is provided with the license key. All universal temporary license keys have an expiration date after which the license can no longer be installed on any unit.

Temporary and universal temporary licenses for Brocade 7810 Extension Upgrade are supported with FOS v8.2.2 or later. Temporary and universal temporary license for Extension Upgrade do not enable additional ports on 7810.

Chapter 12: Hardware Support

12.1 Supported Devices

The following devices are supported in this release:

- 6505, 6510, 6520, DCX 8510-4, DCX 8510-8
- M6505, 6542, 6543, 6545, 6546, 6547, 6548, 6558
- 7840

Use of this Fabric OS release on a switch that has reached its end of support date will result in restricted use of some support level functions. Firmwaredownload, SupportSave and other support commands will not be available. All other basic operational capabilities will be unaffected.

12.2 Supported Blades

12.2.1 DCX 8510-8/DCX 8510-4 Blade Support

Fabric OS 8.2 software is fully qualified and supports the blades for the DCX 8510-8 and DCX 8510-4 as noted in the following table:

Blades	OS Support
FC16-32, FC16-48 16G FC blades	Supported.
FC16-64 blade[1, 2]	Supported.
FC8-64 64-port 8-Gb port blade	Not supported.
FC8-32E, FC8-48E	Not supported.
FCIP/FC Router blade (FR4-18i)	Not supported.
Virtualization/Application blade (FA4-18)	Not supported.
Encryption blade (FS8-18)	Not supported.
Extension blade (FX8-24)	Supported. Up to a maximum of four blades of this type.
FCoE/L2 CEE blade FCOE10-24	Not supported.

[1] 8510 core blade QSFPs, part numbers 57-1000267-01 and 57-0000090-01, are not supported in the FC16-64. The QSFPs supported in the FC16-64, part number 57-1000294-02, is supported on 8510 core blades.
[2] E_Port connections on the FC16-64 blade have the following restriction: connecting a QSFP port between an FC16-64 blade and an ICL QSFP port on a core blade is not supported.

12.3 Supported Power Supplies

12.3.1 DCX 8510-8 Power Supply Requirements

12.3.1.1 Typical Power Supply Requirements for Blades in DCX 8510-8 Backbones

(For a specific calculation of power draw with different blade combinations, see Appendix A, Power Specifications, in the *Brocade DCX 8510-8 Backbone Hardware Reference Manual.*)

Configured Number of Ports	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant Configurations)	DCX 8510-8 @200–240 VAC (Redundant Configurations)	Comments
Any combination of 8-Gb or 16-Gb ports with QSFP ICLs	FC16-32, FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies
256 16-Gb ports + QSFP ICLs	FC16-32, FC16-48 (Maximum of fully populated FC16-32 blades), FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies Max 8 FC16-32 port blades
192 16-Gb ports & max 2 intelligent blades (FX8-24) with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies Max four FC16-48 port blades and max 2 intelligent blades
336 16-Gb ports + QSFP ICLs	FC16-48 (Maximum of seven FC16-48 blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies Max 7 FC16-48 port blades
384 16-Gb ports + QSFP ICLs	FC16-48	Port Blade	Not Supported	4 Power Supplies	200–240 VAC: For DCX 8510-8, four (2+2)[3] 220 VAC Power Supplies are required.
384 16-Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[1] Power Supplies
Any combination of 8-Gb or 16-Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FX8-24	Intelligent Blade / Combination	Dependent on the configuration. Requires a power calculation for the specific configuration.	2 or 4 Power Supplies, depending on the configuration	For DCX 8510-8, four (2+2)[3] 220 VAC Power Supplies are required when any special-purpose blades are installed.

[3] When a 2+2 power supply combination is used, the users are advised to configure the MAPS setting for switch Marginal State to be one Bad Power Supply.

Configured Number of Ports	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant Configurations)	DCX 8510-8 @200–240 VAC (Redundant Configurations)	Comments
512 16-Gb ports	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies
512 16-Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2[3] Power Supplies

12.3.2 DCX 8510-4 Power Supply Requirements

12.3.2.1 Typical Power Supply Requirements for Blades in DCX 8510-4 Backbones

(For a specific calculation of power draw with different blade combinations, refer to Appendix A, Power Specifications, in the *Brocade DCX 8510-4 Backbone Hardware Reference Manual.*)

Configured Number of Ports	Blades	Type of Blade	DCX 8510-4 @110 VAC (Redundant Configurations)	DCX 8510-4 @200–240 VAC (Redundant Configurations)	Comments
96 ports max with QSFP ICLs	FC16-32	Port Blade	2 Power Supplies	2 Power Supplies	1+1 redundancy with 110 or 200–240 VAC power supplies
Any combination of 8-Gb or 16-Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24	Intelligent Blade / Combination	Not Supported	2 Power Supplies	200–240 VAC: 1+1 Power Supplies

12.3.3 Supported Optics

For a list of supported fiber-optic transceivers that are available from Brocade, refer to the latest version of the *Brocade Transceiver Support Matrix* available online at www.broadcom.com.

Note: In FOS 8.2.1 and later, the port speed configuration and SFP speed must match for WAN interfaces to come online on Extension platforms. See Extension for details.

Chapter 13: Software Upgrades and Downgrades

13.1 Platform Specific Downloads

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form. FOS PSD releases provide a smaller version of the FOS image that can only be loaded on a single hardware platform, consisting of a single switch model or group of switch models. These FOS PSD images enable much faster download and file transfer times since they are between 65-90% smaller in size than traditional full FOS images.

Unlike traditional FOS release images that can be installed on any supported Brocade switch and director, FOS PSD images must be downloaded separately for each platform that the FOS release will be used on. The full list of unique FOS PSD images available for this release and the models that each PSD image supports is noted in section Image Filenames.

13.1.1 Using FOS PSDs

FOS PSD images are generally used in the same manner as traditional full FOS release images.

Once loaded onto a switch, the FOS image running is identical to what would be in use if a traditional full image was used for the installation. Issuing a `firmwareshow` command on a switch will display only the FOS version level, with no indication of whether the code was loaded from a FOS PSD image or a full FOS image.

13.1.2 Loading FOS PSDs via Web Tools or FOS Command Line

Installing a FOS PSD image on a switch is performed in the same manner as using a traditional full FOS image. If a FOS PSD image is loaded on an incorrect switch model (for example, attempting to load a FOS PSD image for a Gen 6 entry level switch on a Gen 6 Director), the following error message displays:

> Cannot download the requested firmware because the firmware doesn't support this platform. Please enter another firmware.

13.1.2.1 Loading FOS PSDs via Brocade SANnav Management Portal

Brocade SANnav Management Portal version 2.1.1 or earlier does not support FOS PSD images. However, FOS PSD images are supported with SANnav 2.1.1.3 and later releases. SANnav 2.1.1.3 and later can both host and install FOS PSD images onto Brocade switches.

13.2 Image Filenames

Download the following images from https://support.broadcom.com/.

Fabric OS v8.2.3d

Image Filename	Description
v8.2.3d.md5	Fabric OS v8.2.3d Checksum
v8.2.3d_all_mibs.tar.gz	Fabric OS v8.2.3d MIBs
v8.2.3d_EXT.tar.gz	Fabric OS v8.2.3d for Linux to install on 7840 platforms
v8.2.3d_EXT.zip	Fabric OS v8.2.3d for Windows to install on 7840 platforms
v8.2.3d_pha.tar.gz	Fabric OS v8.2.3d for Linux to install on 6547 platforms
v8.2.3d_pha.zip	Fabric OS v8.2.3d for Windows to install on 6547 platforms
v8.2.3d_G5_ENTRY.tar.gz	Fabric OS v8.2.3d for Linux to install on 6505 platform
v8.2.3d_G5_ENTRY.zip	Fabric OS v8.2.3d for Windows to install on 6505 platform
v8.2.3d_G5_MID.tar.gz	Fabric OS v8.2.3d for Linux to install on 6510 platform
v8.2.3d_G5_MID.zip	Fabric OS v8.2.3d for Windows to install on 6510 platform
v8.2.3d_G5_ENTP.tar.gz	Fabric OS v8.2.3d for Linux to install on 6520 platform
v8.2.3d_G5_ENTP.zip	Fabric OS v8.2.3d for Windows to install on 6520 platform
v8.2.3d_G5_DIR.tar.gz	Fabric OS v8.2.3d for Linux to install on DCX 8510-8, DCX 8510-4platforms
v8.2.3d_G5_DIR.zip	Fabric OS v8.2.3d for Windows to install on DCX 8510-8, DCX 8510-4 platforms
v8.2.3d_EMB.tar.gz	Fabric OS v8.2.3d for Linux to install on M6505, 6543, 6542, 6545, 6546, 6548 and 6558 platforms
v8.2.3d_EMB.zip	Fabric OS v8.2.3d for Windows to install on M6505, 6542, 6543, 6545, 6546, 6548 and 6558 platforms
v8.2.3d_releasenotes_v1.0.pdf	Fabric OS v8.2.3d Release Notes

The image files can be downloaded from https://support.broadcom.com/, with the exception of YANG files which are available on https://www.broadcom.com.

13.3 Migration Path

This section contains important details to consider before migrating to or from this FOS release.

13.3.1 Migrating from FOS 8.2

Any Brocade platform running FOS 8.2.0 or later can be non-disruptively upgraded to FOS 8.2.3d.

13.3.2 Migrating from FOS 8.1

Any Brocade platform running FOS 8.1.0a or later can be non-disruptively upgraded to FOS 8.2.3d.

On Brocade G610, nondisruptive firmware upgrade from FOS 8.1.0 to FOS 8.2.3d is not supported.

13.3.3 Migrating from FOS 8.0

Any Brocade platform and supported blades in the **DCX 8510-8/DCX 8510-4 Blade Support** table and the **X6-8/X6-4 Blade Support** table running any FOS 8.0 firmware must be upgraded to FOS 8.1.x firmware before it can be non-disruptively upgraded to FOS 8.2.3d.

13.4 Upgrade/Downgrade Considerations

Any firmware activation on a DCX 8510-8 or DCX 8510-4 with an FX8-24 blade installed will disrupt I/O traffic on the FCIP links.

Disruptive upgrades to Fabric OS 8.2.3d are allowed and are supported from FOS 8.0.x (up to a two-level migration) using the optional `-s` parameter with the `firmwaredownload` command.

Firmware downgrades from FOS 8.2.3d to FOS 8.2.0x or earlier versions on the Brocade G610 or 6505 are not allowed.

Firmware downgrade from FOS 9.0.0, 9.0.0a, and 9.0.0b to FOS 8.2.3x is not allowed. A workaround is to upgrade to FOS 9.0.1 first then to downgrade to FOS 8.2.3x. There is no such limitation on upgrade.

Chapter 14: Limitations and Restrictions

This chapter contains information that you should consider before you use this Fabric OS release.

14.1 Scalability

All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of this version of the Fabric OS software. For current scalability limits for Fabric OS software, refer to the *Brocade SAN Scalability Guidelines for Brocade Fabric OS 8.X* document.

14.2 Compatibility/Interoperability

14.2.1 Brocade SANnav Management Portal Compatibility

Brocade SANnav Management Portal and Global View are new SAN management software offerings for Brocade SAN environments. There are two distinct SANnav product offerings:

- Brocade SANnav Management Portal
- Brocade SANnav Global View

Brocade SANnav Management Portal allows management of one or more SAN fabrics that are in the same or different geographical locations and supports up to a maximum of 15,000 (15K) physical SAN ports. For environments that are larger than 15K ports, users can deploy multiple SANnav Management Portal instances.

Brocade SANnav Global View is a higher-level management application that provides visibility, summarization and seamless navigation across multiple SANnav Management Portal instances. Users can drill-down to any individual SANnav Management Portal instance from SANnav Global View to perform detailed monitoring, investigation, and troubleshooting.

The SANnav Management Portal 2.0.x supports managing SAN switches running Fabric OS up to v8.2.2x. Compatibility with FOS versions can be found in the SANnav Management Portal 2.0.x Release Notes. FOS v8.2.2a and later require FOS EULA acceptance during firmware migration. The SANnav Management Portal 2.0.x does not support firmware migration from FOS v8.2.2a and later to any FOS version. Use the SANnav 2.1 Management Portal 2.1.x for firmware migration. Alternatively, use WebTools or the CLI in FOS v8.2.2a or later for firmware migration.

14.2.2 Web Tools Compatibility

Fabric OS 8.2.2a is qualified and supported with Oracle Java version 8 update 202. See the “Important Notes” section for more details.

NOTE Microsoft Edge version 79 and later (Chromium-based) is not supported with Web Tools.

14.2.3 SMI Compatibility

It is important to note that host SMI-S agents cannot be used to manage switches running Fabric OS 8.2.2a. If you want to manage a switch running Fabric OS 8.2.2 using the SMI-S interface, you must use SMI agent integrated in either Professional Plus or Enterprise edition of Brocade Network Advisor.

14.2.4 Fabric OS Compatibility

- The following table lists the earliest versions of Brocade software supported in this release, that is, the *earliest* supported software versions that interoperate. Use the *latest* software versions to get the greatest benefit from the SAN.
- To ensure that a configuration is fully supported, always check the appropriate SAN, storage, or blade server product support page to verify support of specific code levels on specific switch platforms before installing on your switch. Use only Fabric OS versions that are supported by the provider.
- For a list of the effective end-of-life dates for all versions of Fabric OS software, visit the following Brocade website: https://www.broadcom.com/support/fibre-channel-networking/eol.
- Gen 6 platforms are supported from FOS v8.2.0 through v8.2.3c only.

Supported Products	Fabric OS Interoperability
Brocade 5424, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480	7.4.2 or later
Brocade 300	7.4.2 or later
Brocade 7800	7.4.2 or later
Brocade DCX 8510-8/DCX 8510-4	FOS 8.2.0 or later
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS 8.2.0 or later
Brocade 6505, 6510, 6520, 7840	FOS 8.2.0 or later
Brocade 6542	FOS 8.2.0 or later[6]
Brocade 6543	FOS 8.2.0 or later
Brocade 6547, 6548, M6505, 6545, 6546	FOS 8.2.0 or later
Brocade 6558	FOS 8.2.0 or later[4]
Brocade G610	FOS 8.2.0 or later
Brocade G620	FOS 8.2.0 or later
Brocade G630	FOS 8.2.0 or later
Brocade 7810	FOS 8.2.1 or later
Brocade X6-8/X6-4	FOS 8.2.0 or later
Brocade X6-8/X6-4 with FC32-48 blade or SX6 blade	FOS 8.2.0 or later
Brocade X6-8/X6-4 with FC32-64 blade	FOS 8.2.0 or later

14.2.5 SNMP Support

Fabric OS 8.2.3 documents the supported MIBs in the *Brocade Fabric OS MIB Reference Manual*. For information about SNMP support in Fabric OS software and how to use MIBs, refer to the *Brocade Fabric OS Administration Guide* for Fabric OS 8.2.2.

[4]Support merged from embedded FOS releases.

14.2.5.1 Obtaining MIBs

You can download the MIB files required for this release from the Downloads area of the Broadcom support portal. To download the Brocade-specific MIBs, you must have a user name and password.

Perform the following steps.

1. Go to https://support.broadcom.com/, click **Login**, and enter your username and password.

   If you do not have an account, click **Register** to set up your account.
2. Select **Hardware > Brocade Storage Networking > My Downloads**.
3. Navigate to the FOS PSD image for your Brocade platform.
4. Navigate to the link for the MIBs package and download the file to your drive.

Distribution of standard MIBs has been stopped. Download the required standard MIBs from the http://www.oidview.com/ or http://www.mibdepot.com/ or https://www.simpleweb.org/ietf/mibs/.

14.2.6 REST API Support

Fabric OS 8.2.3c documents the supported REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

14.2.6.1 Obtaining YANG Files

YANG is a standard data modelling language that defines the data sent over the FOS REST API. Each FOS REST API module is defined in a YANG module file with a .yang name extension.

To download the Brocade FOS-specific YANG files go to https://www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system.

Alternatively, download the YANG files for a specific FOS version from https://github.com/brocade/yang

14.3 Important Notes

14.3.1 System Security

FOS v8.2.3d includes the following enhancements and support updates:

- Support single bind for LDAP login

  The following Microsoft LDAP versions are supported:

  - Windows Server 2019, schema 88 -with certificate support
  - Windows Server 2022, schema 88 -with certificate support

  Support for previous versions of Microsoft LDAP is deprecated in FOS v8.2.3d.

14.3.2 FCoE

The following topologies for FCoE on the FC32-64 are not supported with FOS 8.2.2 or later:

- Cisco UCS server directly connected to the FC32-64 without a Fabric Interconnect module.
- Cisco UCS server with a Fabric Interconnect module connected to the FC32-64 via a Nexus 5000 series switch in between. Neither running FCoE NPV mode nor L2 switching mode on the Nexus 5000 is supported.

14.3.3 FC-NVMe

- FOS 8.1.0 or later is required to support FC-NVMe devices.
- FOS 8.2.1 or earlier does not support FC-NVMe over FCR configurations. FOS 8.2.1b supports FC-NVMe in edge fabric to edge fabric over FCR configuration.

14.3.4 In-flight Encryption and Compression

- FOS 8.2 supports in-flight encryption and compression on the Brocade 6510, 6520, DCX 8510, G620, G630, and FC32-48 port blade. In-flight encryption or compression on the Brocade G620 and G630 is supported with FOS 8.2.0a or later.
- To enable in-flight encryption on the Brocade G620, SFP ports 44 to 47 must be disabled. If ports 44 to 47 have been configured for in-flight compression with FOS 8.1.x or earlier, a firmware upgrade to FOS 8.2.0a or later will be blocked until in-flight compression is moved to other ports in the switch.
- FOS 8.2.1a or later is required to support trunking for encryption ports on the FC32-48 port blade.
- Firmware upgrade to FOS v8.2.2 or later with encryption ports enabled on FC32-48 blade is nondisruptive.

14.3.5 VM Insight

- VM Insight is supported on the Brocade G610, G620, G630, and X6 running FOS 8.1.0 and later. Brocade Gen 5 Fibre Channel platforms support frames with the optional FC Application Header for VM Insight to pass through. The Brocade 7840 and SX6 running FOS 8.1.0 support the Application Header in the FCP emulating tunnel. The FCP emulating tunnel or FICON emulation is not supported in other extension platforms or earlier firmware. Nonemulating tunnel on extension platforms support pass through of the Application Header.
- VM Insight is not supported across FCR, but frames with the Application Header may traverse through FCR.
- FOS 8.2.0 supports VM performance metrics in flows on the ingress F_Port only. The Brocade G610 and G620 support FC metrics. Brocade X6 Directors support both FC metrics and SCSI IO metrics.
- Legacy static flow does not monitor SCSI IOPS statistics for frames with the Application Header.
- Duplicate subflow entries are displayed after a switch HA failover or multiple restarts of VM traffic without clearing the status. The workaround is to use the `flow --reset sys_mon_all_vms` command.
- FOS 8.2.0 does not support VM Insight for FC-NVMe traffic.

14.3.6 ClearLink Diagnostics (D_Port)

- Fabric OS 8.2 supports D_Port tests between two Brocade switches and between Brocade switches and Gen 5 (16Gb/s) and Gen 6 (32Gb/s) Fibre Channel adapters from QLogic and Emulex. The following are specific adapter models and driver versions tested by Brocade with Fabric OS 8.2 for ClearLink.[5]

	Emulex 16G Adapter	Emulex 32G Adapter	QLogic 16G Adapter	QLogic 32G Adapter
Adapter Model	LPe16002B-M6	LPe32002-M2	QLE2672	QLE2742
Adapter Firmware	11.4.204.20	11.4.142.23	v8.05.44	v8.05.44
Adapter Driver	11.4.142.23	11.4.204.8	STOR Miniport 9.1.17.21	STOR Miniport 9.1.17.21

- The D_Port long-duration test can be run only on one port at a time.
- Long-duration electrical loopback tests are not supported.
- D_Port tests on 4x32GFC breakout QSFP optics (P/N 57-1000351-01) and 128GFC non-breakout QSFP optics (P/N 57-1000331-01) have the following restrictions:
- D_Port for these modules in X6 ICL ports is supported without electric or optical loopback tests.
- D_Port on any user port connected by a QSFP require all four user ports within the same QSFP to be in D_Port mode.
- D_Port tests require all user ports in a QSFP to be in the same logical switch.
- Dynamic or On-Demand D_Ports are not supported on the user ports in these modules.
- If a D_Port test between a Brocade switch and an Emulex adapter is stopped shortly after the test has started, the adapter firmware may display "`No FC Cables connecting the port to switch`." The workaround is to restart the D_Port test until completion.
- If a D_Port test is run through optical media for long distance but the ports are not configured for long distance, D_Port test can fail without a pre-check error message about the configuration mismatch.

14.3.7 Forward Error Correction

- FEC is mandatory with Gen 6 Fibre Channel operating at 32Gb/s. This means that the **`portcfgfec`** command applies only to ports that are running at 16Gb/s or 10Gb/s.
- FEC capability is not supported with all DWDM links. This means that FEC may need to be disabled on 16Gb/s or 10Gb/s ports when using DWDM links with some vendors. This is done using the **`portcfgfec`** command. Failure to disable FEC on these DWDM links may result in link failure during port bring-up. Refer to the *Brocade Fabric OS 8.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

14.3.8 Access Gateway

- The 32G links with 4x32G QSFP ports (port 48 to port 63) do not have default mappings. These ports will be disabled by default when a Brocade G620 is enabled for Access Gateway mode or when the configuration is set to the default.
- Attempts to remove failover port mapping from N_Port number 0 on an Access Gateway fail. This problem does not exist on other N_Port numbers.

[5] Adapter firmware or driver versions that are later than the ones listed in the table may not work.

14.3.9 Ingress Rate Limiting

- Fabric OS 8.2 does not support ingress rate limiting on Brocade Gen 6 (G610, G620, G630, or X6) platforms.

14.3.10 Ethernet Management Interface

- The recommended interface speed configuration for a Brocade G620 is 1G auto-negotiate. If a G620 is configured for 10/100M Gb/s forced-speed and fails to establish a link, use a cross-over cable.
- If a Brocade switch management interface is running at 10 Mb/s, certain FOS operations such as **`firmwaredownload`** may fail.
- The 10Gb/s management interface on CPX6 blades is not supported.
- Half-duplex mode are not supported since FOS v8.1.x and is blocked. Firmware upgrade to FOS v8.2.2 is blocked if half-duplex mode is configured.
- External default route to the private IPv4 Class B network of 172.16.0.0/16 is unreachable over the management interface due to the existence of a more specific route from an internal Virtual Fabric ID address of 172.16.0.61/16 for FID 128. The solution is to delete the external default route or change it to a more specific address. The Virtual Fabric address will no longer block management access to the IPv4 Class B address range of 172.16.0.0/16.

14.3.11 Extension

- IP extension (IPEXT) between a Brocade 7840 and an SX6 blade is supported only if the 7840 is running FOS 8.0.2 or later. FCIP extension between a Brocade 7840 with FOS 8.0.2 or later. An SX6 blade with FOS 8.0.2 or later is supported. Extension between a Brocade 7840 or SX6 and a Brocade 7810 is supported only if the 7840 or SX6 is running FOS 8.2.0 or later. The following table documents the combinations.

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware	Supported
7840	8.0.2 or later	7840	8.0.2 or later	Both FCIP and IPEXT traffic
SX6	8.0.2 or later	7840	8.0.2	FCIP traffic but not IPEXT traffic
SX6	8.0.2 or later	7840	8.0.2 or later	Both FCIP and IPEXT traffic
SX6	8.0.2 or later	SX6	8.0.2 or later	Both FCIP and IPEXT traffic
7840	8.2.0 or later	7810	8.2.1 or later	Both FCIP and IPEXT traffic
SX6	8.2.0 or later	7810	8.2.1 or later	Both FCIP and IPEXT traffic

- Do not to configure the HA VE pair (VE16, VE26), (VE17, VE27), (VE18, VE28), and so on, where each VE in the pair is in a different LS with a different traffic policy (port-based routing and exchange-based routing). The workaround is to configure different HA VE pairs such as (VE16, VE27), (VE17, VE26), and so on when putting each VE pair in a different LS with a different traffic policy.
- When Non-Terminate TCP (NT-TCP) is enabled on traffic control lists (TCLs) and a firmware downgrade to FOS 7.4.1d is attempted on the Brocade 7840, the downgrade will be blocked. Users must remove NT-TCP from the TCLs with NT-TCP enabled in order to downgrade the firmware. After the firmware is downgraded to FOS 7.4.1d, users can re-enable the NT-TCP flag.
- Nondisruptive firmware downloads for IP extension support nondisruption to IP traffic for all terminate TCP connections. UDP and non-terminate TCP traffic may be disrupted during HCL.
- After firmware downgrade completion, the Brocade 7840 needs a switch reboot and the SX6 needs a blade power-cycle. HCL is not supported on firmware downgrades.
- If a Brocade 7840 or Brocade X6 Director with an SX6 blade in a non-VF is assigned a fabric ID other than 128, then during a heavy traffic load, the back-end ports on the 7840 and SX6 may encounter credit loss, which can result in traffic disruption over the VE ports. This is tracked as Defect 660208.

- If a 10 Gb/s port is configured on a base configuration of Brocade 7810 with FOS v8.2.2 or later without an Extension Upgrade license, users may see configuration replay errors after the firmware on the 7810 is downgraded to FOS v8.2.1x.
- Some 10G SFP's can run at the 1G speed even though FOS 8.2.3 does not support the 1G setting. The unsupported setting causes issues. FOS 8.2.0 added a check to verify that the configured port speed matches the installed SFP; and displays a RASlog message if it does not match. Starting in FOS 8.2.1, when a 10G SFP is placed in a port configured to 1G, FOS displays the RASlog message and does not bring the port online.
  To resolve this issue, you must replace the SFP with a 1G SFP; or configure the port speed to 10G to match the SFP speed.
- Some 10G SFP's are able to run at 1G speed even though the setting is not supported. This was causing issues. In FOS 8.2.0 a check was added to verify the configured port speed matches the installed SFP and display a raslog message if it does not.

  Starting from FOS 8.2.1 the messages will be displayed, and the port is not brought online when a 10G SFP is placed in a port configured to 1G.

  The resolution is to replace the SFP with a 1G SFP or configure the port speed to 10G to match the SFP speed.

14.3.12 Brocade Analytics Monitoring Platform

- FOS 8.2.0 and later support vTap on Brocade Gen 5 and Gen 6 platforms to be monitored by the Brocade Analytics Monitoring Platform. The supported Brocade platforms include: 6505, 6510, 6520, DCX 8510, 6543, 6545, 6546, 6547, 6548, M6505, 6558, G610, G620, G630, X6.
- vTap is not supported on QSFP ports (port 96 to 127) on the Brocade G630 in Virtual Fabric (VF) mode. It is supported in non-VF mode only.
- If QSFP ports (port 96 to 127) on a Brocade G630 switch are part of the sys_analytics_vtap flow definition, the mirrored frames from these QSFP ports will be discarded for some duration after an HA reboot or after a sys_analytics_vtap flow de-activation.
- The Analytics Switch Link (ASL) connection is not supported on QSFP ports (port 96 to 127) on the Brocade G630. Enabling ASL on these ports will segment the link.
- vTap and auto-discovered AF_Ports do not support high availability. In the event that an AF_Port is rediscovered by a fabric switch after a domain change on the attached Analytics Monitoring Platform and is followed by a `hafailover` or `hareboot` of the fabric switch, the remote AF_Port information will be stale and vTap flows cannot be activated. In this case, use one of the following workarounds:
- Manually configure the AF_Port after `hafailover` or `hareboot`.
- Disable and then enable the AF_Port on the Analytics Monitoring Platform.
- Deactivate the vTap flow before the firmware download, hafailover, or hareboot, and activate the vTap flow again.
- vTap and CS_CTL are mutually exclusive on a fabric switch. If CS_CTL is enabled on one port, the entire switch cannot enable vTap. An F_Port trunk supporting CS_CTL must have all ports in the trunk group enabling CS_CTL. Similarly, in order to enable vTap, all ports in an F_Port trunk must have CS_CTL disabled. In addition, the master port of a trunk should remain the same between CS_CTL enabling and disabling. If this sequence is not followed, vTap may remain active even after CS_CTL is enabled on an F_Port, or the error message "`Disable QoS zones error`" may be observed when enabling vTap. A suggested method is to use the following sequence:
  1. When enabling CS_CTL mode, enable it on all slave ports, followed by enabling it on the master port, noted as port M.
  2. When disabling CS_CTL mode, disable all active ports in the trunk, except the master port M. Disable CS_CTL mode on port M. Enable all ports in the trunk followed by disabling CS_CTL mode on the remaining ports.
  3. When CS_CTL is enabled on a port without any connection, after rebooting and disabling CS_CTL, vTap cannot be enabled. The workaround is to enable the port as a SIM port after disabling CS_CTL and then to toggle the port and remove the SIM port configuration.

- vTap and in-flight encryption or compression compatibility are supported only on the following platforms: Brocade DCX 8510, X6, G620, G630, and 6520. On DCX 8510 and 6520 platforms, the chassis configuration "vTap and Encryption/Compression Coexistence Mode" must be enabled when ports with vTap enabled and ports with in-flight encryption or compression enabled belong to the same ASICs. Refer to the hardware installation guides for these platforms for the port-to-ASIC mapping boundary.
- When "vTap and Encryption/Compression Coexistence Mode" is enabled, the total IOPS on the same ASIC is limited to 250,000. If the IOPS exceeds the limit, the vTap flow will be deactivated.
- When "vTap and Encryption/Compression Coexistence Mode" is enabled, the effective default zone access mode must not be "All Access."
- Running the **`flow --show sys_analytics_vtap`** command when vTap and QoS High compatibility mode is enabled but the vTap flow is not active may display the following message incorrectly: "`Enable vTap and QoS High Priority Zone Compatibility Mode to active vTap flow. Please use the configurechassis command to enable this compatibility mode.`" This is tracked as Defect 604429.
- After a `configuredownload` followed by `switchenable` or a flow statistics reset on the Brocade X6 and G620, MAPS may incorrectly report a VTAP IOPS > 250,000 violation.
- AMPOS 2.2.0 or later is required to support FC32-64 blades. Users should upgrade the Brocade Analytics Monitoring Platform to AMPOS 2.2.0 or later before adding FC32-64 blades to the X6.

14.3.13 Flow Vision

- Flow Vision supports only logical group names that begin with alphabetic characters.
- Frame count statistics of a Flow Monitoring flow may stop incrementing after a **`statsclear`** command. To work around the problem, users may run the **`slotstatsclear`** command. To recover from such condition, complete the following steps:
  a. Disable all flows in the logical switch.
  b. Delete the problem flow.
  c. Create a new flow to replace the problem flow.
  d. Activate the new replacement flow.
  e. Verify the new replacement flow.
  f. Enable all other flows.
- IO Insight metrics are supported on ingress and egress ports on the Brocade X6 and on egress ports on Brocade G620 and G630 switches. They are not supported on Brocade G610 switches.
- Activating a Flow Monitoring flow on an egress port on the Brocade G610 with the **`-frametype`** parameter may cause a resource not available error.
- FC-NVMe flow IO Insight metrics are supported with a Flow Monitoring flow on a port defined on the Brocade G630 and FC32-64 blade only. Users must use the **`-nsid`** parameter with the **`flow --create`** command to monitor FC-NVMe flows. Either a valid Name Space ID (NSID) must be used or the `all` keyword must be used to select all valid NSIDs.
- When a flow is created with the **`-frametype`** parameter, FC-NVMe traffic is included in the metrics for the following SCSI frame types: SCSI, SCSITur, SCSIXferrdy, and SCSIGoodStatus.
- Flow Mirroring is not supported on QSFP ports (port 96 to 127) on the Brocade G630 with Virtual Fabric (VF) mode. It is supported in non-VF mode only.
- Mirror ports are not supported on QSFP ports (port 96 to 127) on the Brocade G630. Enabling a mirror port on these ports will disable the ports.
- If a flow is imported to MAPS and configured with incorrectly configured flow metrics thresholds, a high frequency violation of the thresholds may result in very slow display of the RASLOG alerts for the violations.

14.3.14 FICON

For FICON-qualified releases, refer to the Additional Considerations for FICON Environments section of the Appendix for details and notes on deployment in FICON environments. (This appendix is included only for releases that have completed FICON qualification.)

14.3.15 MAPS

MAPS monitoring of UCS server login does not support the FENCE action even though the **mapsrule** command does not block the configuration.

14.3.16 Miscellaneous

- If the ambient temperature is above the recommended operational limit, the power supply units may shut down, in particular when the ambient temperature is above 62°C for Brocade X6 Directors. This will result in the switch being shut down without any warning. Refer to the *Brocade G620 Hardware Installation Guide* and the *Brocade X6-8/X6-4 Hardware Installation Guide* for the recommended ambient temperature limits for the switches.
- After a power supply unit is removed from a Brocade G620, the **historyshow** command may miss the entries for this FRU removal or insertion event. In addition, the RASLog error message EM-1028 may be logged when the power supply is removed. This condition can be corrected by power-cycling the switch.
- After running offline diagnostics mode 1 on QSFP ports, a Brocade G620 must be rebooted before operational use.
- All links in an ICL QSFP connection on a Brocade X6 Director must be configured to the same speed using the **portcfgspeed** command from one of the following supported speeds: 16Gb/s, 32Gb/s, or ASN. To connect an ICL from an X6 with a 4x32GFC breakout optic (P/N 57-1000351-01) or a 4x16G FC optic to a 4x16G FC optic in a DCX 8510, the X6 port's speed must be set to 16Gb/s.
- ASN is not supported with 4x32GFC breakout optics (P/N 57-1000351-01).
- When connecting 4x32G FC breakout optics (P/N 57-1000351-01) to 32Gb/s SFP peer ports on Gen 6 platforms, ports may auto-negotiate to 16Gb/s after **switchdisable** and **switchenable** on the Gen 6 platforms with 32Gb/s SFP ports. To avoid this issue, the Gen 6 platforms with 32Gb/s SFPs should be upgraded to FOS 8.2.0 or later or to FOS 8.1.2b or later. This issue is more likely to occur when the Gen 6 platforms with 32Gb/s SFPs are X6 directors.
- Brocade G630 LEDs illuminate amber and green during power-up.
- When launching Web Tools over an HTTPS connection and a security warning message for an untrusted certificate pops up, the pop-up message should be responded to within 20 seconds.
- When replacing a FC32-64 blade with a FC32-48 blade, flexport and FCoE configurations should be removed before the FC32-64 blade is removed.
- In ISL between G720 or FC64-48 (64G optic) to a G630 (32G optic) may take longer to converge at 32G speed. This is applicable when the G630 switch is running pre-FOS 9.0.1. Upgrade the G630 to FOS 9.0.1 or later when connecting a G630 to a G720 or FC64-48.
- The output of CLI command `sfpShow` or any other interfaces to retrieve information from 32Gb/s 100m QSFP (Part Number 57-1000490) does not match the Part Numbers on the media sticker labels. The output shows Part Number 57-1000351 instead. This does not affect operation of the optics.

Chapter 15: Security Vulnerability Fixes

This section lists the Common Vulnerabilities and Exposures (CVEs) that have been addressed. Each CVE is identified by the CVE ID number. For the latest security vulnerabilities disclosures and a description of each CVE, please visit Brocade Security Advisories web page at https://www.broadcom.com/support/fibre-channel-networking/security-advisories

Brocade Fabric OS version 8.2.3d

CVE-2023-31426

CVE-2022-0778

CVE-2018-7738

CVE-2021-39275

CVE-2018-0739

CVE-2022-24448

CVE-2020-36557

CVE-2020-36558

CVE-2018-14404

Brocade Fabric OS version 8.2.3c1 and 8.2.3d

CVE-2022-33186

A vulnerability in Brocade Fabric OS software v9.1.1, v9.0.1e, v8.2.3c, v7.4.2j and earlier versions could allow a remote unauthenticated attacker to execute on a Brocade Fabric OS switch commands capable of modifying zoning, disabling the switch, disabling ports and modifying the switch IP address.

Brocade Fabric OS version 8.2.3c

CVE-2022-28169

A configuration option to prevent a low privilege webtools user from gaining elevated admin rights, or privileges, beyond what is intended or entitled for that user. By exploiting this vulnerability, a user whose role is not an admin, can create a new user with an admin role using the operator session id. The issue was replicated after intercepting the admin and operator authorization headers sent unencrypted and editing a user addition request to use the operator's authorization header.

CVE-2022-28170

Brocade Fabric OS Web Application services before Brocade Fabric v9.1.0, v9.0.1e, v8.2.3c, v7.4.2j stores server and user password in the debug statements.

CVE-2022-33179

A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 7.4.2j could allow an attacker to break out of restricted shells with “set context” and escalate privileges.

CVE-2022-33180

A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, could allow an attacker to export out sensitive files with “seccryptocfg”, “configupload”.

CVE-2022-33181

An *information disclosure* vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow an attacker to read sensitive files using switch commands “configshow” and “supportlink”.

CVE-2022-33182

A privilege escalation vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, could allow a local user to escalate its privilege to root using switch commands “supportlink”, “firmwaredownload”, “portcfgupload, license, and “fosexec”.

CVE-2022-33183

A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow an attacker to perform stack buffer overflow using in “firmwaredownload” and “diagshow” commands.

CVE-2022-33184

A vulnerability in Brocade Fabric OS fab_seg.c.h libraries could allow authenticated attackers to exploit stack-based buffer overflows, allowing the execution of arbitrary code as the root user account.

CVE-2018-0732

During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

CVE-2019-9169

In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.

CVE-2021-39275

ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party/external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVE-2021-34798

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVE-2021-23841

The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

Brocade Fabric OS version 8.2.3b

There are no new CVEs for 8.3.2b

Brocade Fabric OS version 8.2.3a

CVE-2021-27794

A vulnerability in the authentication mechanism of Brocade Fabric OS versions before Brocade Fabric OS v.9.0.1a, v8.2.3a and v7.4.2h could allow a user to Login with empty password, and invalid password through telnet, ssh and REST.

CVE-2021-27793

Intermittent authorization failure seen with aaa tacacs+ can cause a user with a valid account to be unable to log into the switch. Observed on FOS firmware before Brocade Fabric OS v9.0.1b and after 9.0.0. Also observed on FOS firmware before Brocade Fabric OS v8.2.3a and after v8.2.0.

CVE-2021-27792

The request handling functions in web management interface of Brocade Fabric OS versions before v9.0.1a, v8.2.3a, and v7.4.2h do not properly handle malformed user input, resulting in a service crash. An authenticated attacker could use this weakness to cause the FOS HTTP application handler to crash, requiring a reboot.

CVE-2021-27791

The function that is used to parse the Authentication header in Brocade Fabric OS Web application service before Brocade Fabric OS v9.0.1a and v8.2.3a fails to properly process a malformed authentication header from the client, resulting in reading memory addresses outside the intended range. An unauthenticated attacker could discover a request, which could bypass the authentication process.

CVE-2020-15388

The Web application of Brocade Fabric OS before versions Brocade Fabric OS v9.0.1a and v8.2.3a contains debug statements that expose sensitive information to the program's standard output device. An attacker who has compromised the FOS system may utilize this weakness to capture sensitive information, such as user credentials.

CVE-2020-15386

Brocade Fabric OS prior to v9.0.1a and 8.2.3a and after v9.0.0 and 8.2.2d may observe high CPU load during security scanning, which could lead to a slower response to CLI commands and other operations.

- Base Score: 5.3 Medium
- Products Affected: Brocade Fabric OS versions after v9.0.0 and before v9.0.1a, and Brocade Fabric OS versions after v8.2.2d and before v8.2.3a
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE-2020-1971

The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools.

CVE-2019-11479

Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11.

Brocade Fabric OS version 8.2.3

CVE-2021-27792

The request handling functions in web management interface of Brocade Fabric OS versions before v9.0.1a, v8.2.3a, and v7.4.2h do not properly handle malformed user input, resulting in a service crash. An authenticated attacker could use this weakness to cause the FOS HTTP application handler to crash, requiring a reboot.

CVE-2021-27790.

The command “ipfilter” in Brocade Fabric OS uses unsafe string function to process user input.

CVE-2021-27789.

A vulnerability in the Brocade Fabric OS could allow an authenticated CLI user to abuse the history command to write arbitrary content to files.

CVE-2021-3449

An OpenSSL TLS Server may crash if sent a maliciously crafted renegotiation ClientHello message from a client.

CVE-2018-6449

Host Header Injection vulnerability in the http management interface in Brocade Fabric OS versions before v9.0.0 could allow a remote attacker to exploit this vulnerability by injecting arbitrary HTTP headers.

Chapter 16: Defects

16.1 Closed with Code Changes in 8.2.3d

Defect ID:	FOS-806174		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.1.0 (EOS)	**Technology:**	Zoning
Symptom:	Duplicate member are allowed for a peer zone via GUI and CLI by different alias; However, switch loss HA sync after user created alias with same member.		
Condition:	When user create alias peer zone having duplicate members across principal and peer members.		
Workaround:	Make sure no duplicate member entries during alias creation.		
Recovery:	After removing duplicate member entries via aliremove and cfgsave, sync can be attained through hadisable and haenable or standby CP reboot.		

Defect ID:	FOS-810478		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1b	**Technology:**	High Availability
Symptom:	Switch HA out of sync in VF configuration.		
Condition:	When an invalid port mappings in the VF configuration file is synced to the standby CP, buffer overrun would happen and HASM would terminate. This applies to pre-FOS9.0.0 releases.		

Defect ID:	FOS-824498		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS

Reported In Release:	FOS8.2.2c	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	MAPS test email defaulted "From address" to root@switchname.domain.com on some switches and rejected by postmaster.		
Condition:	The "From address" in the SMTP header was not properly intialized.		

Defect ID:	FOS-827306		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1b	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	Repeated XTUN-1997 RASLOGs generated in an Extension configuration through a 7810, 7840 or SX6 blade that may or may not be associated with a VE port down event. The specific trigger is: ttmh0933|tifa1243| timer [1] reset error		
Condition:	WAN TCP timer reset failure. This could cause a failure and closure of a WAN TCP circuit. FCIP Tunnel will attempt to close and then re-open a new TCP connection.		
Recovery:	FCIP Tunnel will auto attempt to close and then re-open a new TCP connection.		

Defect ID:	FOS-829100		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.3c	**Technology:**	Zoning
Symptom:	Path unstable when zone miss counter increases but the cam entries are verified to be good. Plogi ack , abts frames are dropped.		
Condition:	Happens when ports are moved out of a LS and then switchdisable is performed on the LS.		
Recovery:	Power cycle the slot with the affected ports or cold boot the switch.		

Defect ID:	FOS-832909		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.1.0	**Technology:**	Name Server
Symptom:	FCR (iSwitchd) uses RSCNs to convey incremental updates to the device directory. When an RSCN fails to be delivered, the Name Server database can become out of sync across routed fabrics.		
Condition:	When iswitchd does not receive both RSCN ACCept and ACK_1, the re-tries made could go out-of-order.		

Defect ID:	FOS-838584		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3c	**Technology:**	Management GUI
Symptom:	Weblinker termination due to segmentation fault.		
Condition:	During MAPS dashboard summary data query.		

Defect ID:	FOS-839810		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.1b	**Technology:**	Firmware upload/download
Symptom:	User may see repeated logging of an internal firmwaredownload raslog messages.		
Condition:	This could happen when there is an unlikely file system error and corrupted firwaredownloadstatus file size goes to zero. Once the file size is zero, the frequency of the internal firmwaredownload raslog messages correspond to the frequency of the invocation of the CLI command firmwaredownloadstatus or the corresponding REST API to fetch firwaredownloadstatus.		

Workaround:	To stop the flooding of the interal raslog, user may run the following command via root access. rm /etc/fabos/upgrade_status1

Defect ID:	FOS-840370		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.3a	**Technology:**	Component
Symptom:	Firmwareupgrade failed due to time-out from a busy standby CP; HA lost sync after cald panic with a large sized core file and high compact flash usage.		
Condition:	This is seen on an ESRS configured director, where standby CP continuously attempts to get the port capabilities causing firmwaredownload to timeout during ESRS report generating. Following messages repeatedly logged on console or via dmesg: "kernel: : IOCTL not allowed: cmd 0x2000455e, pid 2277 (cald) - temporary" This left large /var/log/messages* files on the switch. If there is a hafailover while at this busy standby CP moment, CPs could lost HA sync and cause cold recovery.		
Workaround:	Disable ESRS before upgrade.		

Defect ID:	FOS-841163		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.3	**Technology:**	CLI
Symptom:	User can't perform firmware download on the switch from SANNav.		
Condition:	This issue will be observed when host IP (which is used for performing firmware download) is already present in the SSH known host with custom port number.		
Recovery:	Need to manually login into switch using SSH interface and execute following command "sshutil delknownhost" to delete the host entry from SSH known host.		

Defect ID:	FOS-841254

Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Unexpected reboot or failover after running out of memory.		
Condition:	When user used incorrect credential to perform mib walk and left a large /tmp/snmpd.log file filled with" Authentication failed for snmpadmin1"		
Workaround:	Use correct credential or as root, cat /dev/null > /tmp/snmpd.log before running out of memory.		

Defect ID:	FOS-841520		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.3b	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	Host reboot will trigger MAPs alert Condition=ALL_SFP(RXP<=200), Current Value:[RXP, 2 uW]		
Condition:	After a port state change, such as port offline & online, the SFP values are not yet updated during the polling cycle, but used by MAPs.		

Defect ID:	FOS-842145		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.3b	**Technology:**	Logging
Symptom:	User may encounter VPD write error to WWN card after the system transitions to CF_ACTV state for WWN Data Protection (WDP).		
Condition:	This is applicable only for the DCX-8 and 8510-8 platforms.		

Defect ID:	FOS-843045		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3b	**Technology:**	Management GUI
Symptom:	MAPs alarms continue to be generated following the addition of WWN Data Protection license.		
Condition:	This is applicable to DCX-8 and 8510-8 only, which are the only platforms covered by WWN Data Protection.		

Defect ID:	FOS-843422		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2d	**Technology:**	NPIV - N-Port ID Virtualization
Symptom:	UCS Server FLOGI is being held. Issue doesn't disappear when server is shutdown. Server cannot see paths through this adapter, can only see storage through other Fabric.		
Condition:	After configuring FCoE enodes, doing hafailover, and then removing all FCoE enodes, NPIV device logged in and got the 64th or higher AL_PA on one of the first 16 ports on a 48-port blade on a chassis. Then the same device tried to login again without logging out.		
Recovery:	Disable and then enable the switch port where the device experienced the issue. This is only a temporary recovery because NPIV devices that re-login frequently will eventually hit the issue again.		

Defect ID:	FOS-843463		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.3b	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Getting Alerts for HTTPS SW certificate triggered DAYS_TO_EXPIRE rule - defCHASSISCERT_VALIDITY.		

Condition:	When an old certificate expires, MAPS module continues to maintain the old certificate on the switch and generates a false alarm.
Workaround:	Delete the old expired certificate.

Defect ID:	FOS-843589		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3d	**Technology:**	Management Server
Symptom:	MAPS traps being sent to other monitoring software even though maps rule are configured with action 'NONE'.		
Condition:	MAPS ignores action set to NONE when BNA or SANnav has registered as a trap receiver. The setting for BNA/SANnav monitoring (Second field is 3 in snmp.trapFilter:0,3;) is causing the NONE for SNMP in the MAPS rule to be overridden, resulting in traps being sent		

Defect ID:	FOS-844074		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3d	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Detected termination of process snmpd.		
Condition:	During a 3rd party SNMP application sending SNMP GET requests with invalid port index (swFCPortTable) causing the NULL pointer access.		

Defect ID:	FOS-844942		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.3b	**Technology:**	User Accounts & Passwords

Symptom:	USERID account gets deleted.
Condition:	It impacts BR6547 embedded switch only when user implements the Factory default on chassis management module.

Defect ID:	FOS-845216		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3b	**Technology:**	CLI
Symptom:	User may encounter an unexpected sudden system reboot		
Condition:	This may occur if the user invokes the CLI command "switchviolation --dump -dcc" or executes scripts invoking this CLI command.		

Defect ID:	FOS-845750		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.3c	**Technology:**	Fibre Channel Routing
Symptom:	Support for non-disruptive EX port link cost changes.		
Condition:	Enhance to allow change EX port link cost nondisruptively.		

Defect ID:	FOS-846479		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3d	**Technology:**	Management GUI
Symptom:	Weblinker restart on switch.		
Condition:	This issue is seen when there is HTTPs connection reset.		
Workaround:	User can enable https keepalive using "mgmtapp --enable keepalive".		

Defect ID:	FOS-847045		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.3d	**Technology:**	Port Bring-up
Symptom:	Switch panic is observed when a timer is added before the same exact timer expires.		
Condition:	This condition occurred due to a small timing window where an end device went offline at about the same time as doing a FLOGI or PLOGI.		

Defect ID:	FOS-847171		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.3d	**Technology:**	Port Bring-up
Symptom:	G610 switch state is set to faulty after switchdisable/switchenable. G610:admin> switchshow ... switchType: 170.2 switchState: Faulty switchMode: Native switchRole: Faulty ...		
Condition:	This impacts G610 switch only and it could happen in a timing race condition when the port is bounced while traffic is flowing.		
Recovery:	Power cycle the switch.		

Defect ID:	FOS-847308		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1b	**Technology:**	Platform Services
Symptom:	Brocade 7840 may encounter kernel panic due to OOM, with tunnels failing to come online after reboot		
Condition:	This is triggered as a result of a slow memory leak.		

Defect ID:	FOS-848567		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3d	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	WWN is missing in the oid when run snmpgetnext command to connUnitPortTable.		
Condition:	When run snmpgetnext command to connUnitPortTable in FOS823x, there is no wwn information: connUnitPortPhysicalNumber 1.3.6.1.3.94.1.10.1.18 connUnitPortStatus 1.3.6.1.3.94.1.10.1.7 connUnitPortState 1.3.6.1.3.94.1.10.1.6 connUnitPortType 1.3.6.1.3.94.1.10.1.3 connUnitPortSpeed 1.3.6.1.3.94.1.10.1.15		

16.2 Closed with Code Changes in 8.2.3c

Defect ID:	FOS-800614		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	CLI - Command Line Interface
Symptom:	CLI "nsshow -t" does not list the correct device type (host or target); it shows as "Physical Unknown(initiator/target)".		
Condition:	Run CLI "nsshow -t" on switch with a specific 3rd party device connected.		

Defect ID:	FOS-806884		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1b	**Technology:**	Firmware upload/download
Symptom:	Detected termination of daemons during a non-disruptive firmware upgrade.		
Condition:	A critical race condition during warm code upgrade, when name server daemon starts sending rscns to the application like msd, ficud, appsrv etc. and these applications are not yet ready to receive. It's more likely to happen in a large scale fabric. This only impacts pre-FOS 9.x releases.		

Defect ID:	FOS-821090		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.0a	**Technology:**	Management GUI
Symptom:	weblinkerfcgd core files are generated on the switch.		
Condition:	This issue could be hit on a system configured with multiple Virtual Fabrics when there is an HTTP/HTTPS based client (SANnav,		

	WebEM, REST clients) monitoring the switch at the same time as certificates being installed on the switch.
Workaround:	Stop the HTTP/HTTPS based clients prior to the installation of the certificates from CLI. Once the certificates are installed, the HTTP/HTTPS based management applications can start monitoring the switches.

Defect ID:	FOS-821746		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1c	**Technology:**	Zoning
Symptom:	Edge to edge routing was not working and frames dropped on E-port or EX-port.		
Condition:	A port could be left in a state with a zoning flag set, when it was initially an F-Port and the device had sent a LOGO or quickly went offline. When such a port is moved to a logical switch, which does not have any zoning such as a base switch, and the port becomes an Eport/Export, the issue will be seen on the port.		
Workaround:	Use 'filterportshow' to confirm zoning is disabled before using a port as an E-Port or EX-port.		
Recovery:	Move the port to a logical switch with zoning enabled, enable the port, and then move it back to the original logical switch.		

Defect ID:	FOS-822366		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2a	**Technology:**	Inband Management
Symptom:	cald terminated and kernel paniced during supportsave collections.		
Condition:	Observed during a race condition where cald failed to perform internal common transport registration.		

Defect ID:	FOS-823847

Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS9.0.1	**Technology:**	Component
Symptom:	Switch panic after cald failed to allocate memory for maintaining keep alive with ESRS.		
Condition:	When ESRS is configured.		

Defect ID:	FOS-826227		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.2c	**Technology:**	Zoning
Symptom:	Devices in default allaccess zone cannot communicate to each other across LISLs in FICON environment on all platform.		
Condition:	FICON logical switch with allaccess default zone, no configured zones, and FMS mode enabled. Traffic across LISL is dropped. This should happen only for FOS release 8.2.2c and later, FOS8.2.3, and FOS9.0.0 and later.		
Workaround:	Either disable FMS mode or define zones.		

Defect ID:	FOS-832152		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.2d	**Technology:**	Routing
Symptom:	All hosts on two AGs lost access to storage after ports were added to F-Port trunk group		
Condition:	This is encountered when N-port trunk master changes to a port in the same trunk that has never been an individual N-port or an N-port trunk master since the last cold boot or power cycle.		
Recovery:	Disable all ports in the N-port trunk at the same time, and then enable them again, all at the same time.		

Defect ID:	FOS-832938		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.0.0b	**Technology:**	Frame Redirection
Symptom:	Class 2 Link Control frames (like ACK_1) are dropped.		
Condition:	Happens when the BI link get a LR and during the online state after LR, the FICON CUP DST and the BYpass RAM bit is set.		
Recovery:	Power toggle the blade.		

Defect ID:	FOS-835586		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a	**Technology:**	SNMPv2, SNMPv3 & MIBs
Symptom:	SNMP consumes more CPU cycles, resulting in MAPS alerts.		
Condition:	This issue occurs on platforms where there are no GigE ports or when using a 3rd party monitor application, which performs snmpget via multiple varbinds to FC ports and interface tables, this impacts 32G Gen5 platforms only.		

Defect ID:	FOS-836232		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.1.0	**Technology:**	Configuration Fundamentals
Symptom:	The user will observe that Tunnel with Preshared key will not come up after config download.		
Condition:	A functioning IKE session between switches running different IKE revisions is restarted at the higher revision IKE, after the IKE session has been rekeyed at least once.		

Recovery:	Restart the IKE session at the lower-revision switch.

Defect ID:	FOS-836304		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2c	**Technology:**	Diagnostic Port (D_Port)
Symptom:	Frames to the remote fabric across the IFL are dropped after D-port testing.		
Condition:	The port was first configured as D-port and D-port test was interrupted by disabling the port. The port is then configuraed as IFL port.		

Defect ID:	FOS-836468		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.1.0	**Technology:**	CLI
Symptom:	switchtype command not working on Admin account.		
Condition:	This is encountered when the switchtype CLI command is invoked in Admin account		

Defect ID:	FOS-836506		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.3a1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	Periodic XTUN-1997 triggers when running FICON and FCP/SCSI flows over an FCIP Tunnel Port Based or Device Based Routing configuration. The XTUN-1997 triggers are for Keepalive timeouts on the medium priority circuits.		

Condition:	FCIP Tunnel with FCP/SCSI flows in a non-EBR logical switch. There are times when an FCP/SCSI flow uses the control VTN between the switches. This causes a KATO on the H/M/L active connections.

Defect ID:	FOS-836531		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2d	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	Switch panic with maps daemon (MDD) watchdog timeout.		
Condition:	This may be encountered on a very busy Chassis System. MDD watchdog timeout occurs when it takes too long for mdd to get slot count information on a busy chassis platform.		

Defect ID:	FOS-836572		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.1c	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	'snmpconfig' CLI returns error 'Failed to get snmp config info' due to SNMP service not restarting after getting disrupted.		
Condition:	When 3rd party application polls FC data using SNMP with negative value as port index.		

Defect ID:	FOS-836573		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.3a	**Technology:**	FCIP - Fibre Channel over IP

Symptom:	FICN_1062 and FICN_1063 RASLOGs every 1.5 seconds on FICON Emulation enabled FCIP Tunnel
Condition:	This is seen on XRC FICON Emulation enabled tunnel. If a device presents Attn status that is Idle Status Accepted at the remote site, but then fails to be presented at the host side, and the device re-presents the Attn status when the host side is still in progress, then the second and subsequent Attn status presentations from the device side are aborted by the device.

Defect ID:	FOS-837088		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2d	**Technology:**	Management Server
Symptom:	FOS accepts REST request with an empty audit class list.		
Condition:	Run a REST request to set an empty audit class which should be handled as an invalid input.		

Defect ID:	FOS-837183		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.2d	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	TX rules for ISL ports do not get triggered for MAPS custom policy that includes both RX and TX rules for the ISL ports.		
Condition:	This is specific to Gen 5 stats collection where the stats on the tx utilization is NOT reported back to maps correctly.		

Defect ID:	FOS-837280		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management

Reported In Release:	FOS9.0.1c	**Technology:**	Port Bring-up
Symptom:	Boot over SAN device does not work after upgrading firmware on 32G FC switches.		
Condition:	This is encountered on 32G switches soon after upgrading to FOS8.2.3a, FOS8.2.3b, FOS9.0.1c, FOS9.1.0 and FOS9.1.0a.		
Recovery:	Retry boot over SAN.		

Defect ID:	FOS-837538		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Distance
Reported In Release:	FOS7.4.2g	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	Different (lower) tunnel throughput on 7800 or FX8-24 configuration after reboot or slot power cycle.		
Condition:	After reboot of a 7800 switch or FX8-24 blade, the FCIP data complex could incorrectly setup egress internal FC ports leading to reduced FC throughput.		

Defect ID:	FOS-837583		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a1	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP daemon leaks memory and causes switch to hafailover/hareboot/panic when switch runs out of memory.		
Condition:	Memory leak is observed from SNMP get request for connUnitSNStable objects.		

Defect ID:	FOS-837755		
Technical Severity:	High	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.1.0b	**Technology:**	Name Server / Zoning
Symptom:	Stale CAM entries are present on the ports, which were disabled.		
Condition:	When a port is disabled, the CAM entries on the port are not deleted except for the Loopback CAM pair.		
Recovery:	Poweroff the slot or reboot the switch to recover from this incorrect state.		

Defect ID:	FOS-837837		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.2d4	**Technology:**	Component
Symptom:	Performance stats for VE ports are not present in connunitportstat table		
Condition:	This is observed when using snmpget/snmpwalk to gather VE port stats.		

Defect ID:	FOS-838047		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.0.1b4	**Technology:**	ICLs - Inter-chassis Links
Symptom:	During the FOS upgrade process, initiated from SANnav, directors can experience unexpected reboots during the upgrade process. In each director where this occurred the FOS upgrade had completed on the Standby CP and then an unexpected reboot occurred. Both CR blades reset and started POST diagnostics.		
Condition:	FICON logical switch with 256 ports that are bound to all available areas. ICLs then moved to the FICON logical switch cause VERIFYs and ASSERT upon hafailover.		
Workaround:	Remove two ports bound to areas from the logical switch. Then remove all ICLs from the logical switch and add them back.		

Defect ID:	FOS-838514		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.3a1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	7840, 7810 or SX6 blade encounters DP Linux out of Memory causing IO disruption		
Condition:	FCIP Tunnel down events after many (>> 25,000) FTRACE triggers as indicated by XTUN-1997 RASLOGs.		

Defect ID:	FOS-838549		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.2d	**Technology:**	BB Credits
Symptom:	Loss of paths after hafailover (firmwaredownload).		
Condition:	Class 2 TX credit is lost when the end device delays PLOGI during Class 2 communication, and then hafailover happens twice. This is a new device behavior that exposed a day-1 FOS issue.		
Recovery:	Bounce impact ports with class2 credit dropped to zero.		

Defect ID:	FOS-838915		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.3a2	**Technology:**	Port bring up
Symptom:	Switch panic while processing an incoming Fibre Channel frame.		
Condition:	End device sends an invalid multi-frame sequence to the switch.		

Defect ID:	FOS-838977

Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.1.1	**Technology:**	Web Tools
Symptom:	Weblinkercfg continues crashing while processing Enumerate telemetry profile query.		
Condition:	This occurs when telemetry profile index no longer starts with 0. For example when a user creates 4 profiles and deletes the first 2 profiles, then the remaining two profile index no longer starts at 0. This condition can be simulated by using two Sannav servers simultaneously streaming to kafka brokers.		

Defect ID:	FOS-839056		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.2d	**Technology:**	Routing
Symptom:	Frame drops affecting entire fabric after creating smaller trunks from larger trunks.		
Condition:	This is encountered when a small trunk is created from ports in a larger trunk followed by hafailover.		
Workaround:	Do not use port of larger trunk for the new trunk. Or alternatively, Disable all ports in the larger trunk first and then create the smaller trunk.		
Recovery:	hafailover of the switch showing the drops will recover from this condition.		

Defect ID:	FOS-839186		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.3a	**Technology:**	Web Tools

Symptom:	Code upgrade turned into cold recovery when weblinker cannot restart in time, or on an normal operation switch, user may encounter failures in config change operations (e.g. portcfg or lscfg)
Condition:	This occurs during code upgrade or if config operations are performed within a minute of any operation (e.g. install / remove / modify HTTP certificates etc) that forces a restart of the weblinker.
Workaround:	Upgrade one CP at a time. Upgrade the standby CP 1st and wait for 2-3 mins after HA sync is achieved before failing over to the new firmware. Or Do not make any config changes (e.g portcfg ftrace 3/24 del, etc) for one minute after any operation (e.g. install / remove / modify HTTP certificates etc) that entails a restart of the weblinker

Defect ID:	FOS-839346		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1d	**Technology:**	Routing
Symptom:	Path loss experienced after FOS upgrade on Access Gateway		
Condition:	The Path loss occurs when F-port trunk slave on AG is disabled and followed by an hareboot.		
Recovery:	Bounce the affected host/target devices.		

Defect ID:	FOS-839507		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.2c6	**Technology:**	CLI
Symptom:	Switch fault after Portledtest causing EM-1334 & BL-1020 raslog.		
Condition:	Run CLI Portledtest after firmwaredownlaod on BR7810 platform.		

Defect ID:	FOS-839820		
Technical Severity:	High	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.3b	**Technology:**	Component
Symptom:	Brocade 8510-8 director class switches with a single faulty WWN card, running FOS v8.2.3a or FOS v8.2.3b may encounter a failure reading from the WWN cards.		
Condition:	Brocade 8510-8 director class switches and Brocade DCX-8 Director class switches upgraded to be an 8510-8 running FOS releases v8.3.2a and v8.3.2b.		

Defect ID:	FOS-840010		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.3b	**Technology:**	FC-FC routing
Symptom:	LSAN traffic stopped after adding a new switch to the edge fabric.		
Condition:	When there is no device entry to send to edge fabric, edge fabric switch misinterprets the small compressed GE_PT response payload.		

Defect ID:	FOS-840082		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.3b	**Technology:**	Equipment Status
Symptom:	The following similar raslog may be see without actual excessive power consumption: EM-1230 1 of 3 Excessive Power usage detected PS1(564)+PS2(144)=708W. System will shutdown on consecutive readings above 700W.		
Condition:	This may be seen only on Brocade-6520 platform.		

Defect ID:	FOS-840717		
Technical Severity:	Medium	**Probability:**	Medium

Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3b	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	High CPU usage reported on snmp daemon.		
Condition:	When application query ConnUnit Port table via snmp interface on Gen5 platforms.		

Defect ID:	FOS-840768		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.3a	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	Switch panic when trace module has memory corruptions.		
Condition:	Switch panic when trace module has memory corruptions, and module ID is out of range .		

Defect ID:	FOS-840909		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1c	**Technology:**	Fibre Channel Addressing
Symptom:	FCPH-1003 reports duplicate port WWN with a port that does not have the same port WWN.		
Condition:	This is encountered when many devices are requesting 8-bit area and two such devices come online at the same time vying for the last available 8-bit area.		
Workaround:	Bring devices up one at a time, in a staggered order.		
Recovery:	Re-enable any ports that were disabled.		

Defect ID:	FOS-841141		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2c	**Technology:**	Configuration Fundamentals
Symptom:	MAPS test email using FROM address of "root@switchname.domain.com" which is not always supported.		
Condition:	When sending a test email from switch, enhanced to user "postmaster" instead of "root".		

Defect ID:	FOS-841478		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a	**Technology:**	Fibre Channel Services
Symptom:	Duplicate PWWN detection resulted in disruption to the existing FICON CHPID.		
Condition:	Device logs into a FICON switch with a PWWN that matches the PWWN of another device on the same switch.		
Workaround:	Avoid intentionally logging in devices with duplicate PWWNs.		
Recovery:	Remove devices with duplicate PWWNs and bounce the original devices.		

Defect ID:	FOS-841574		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3b	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	After upgrading to FOS 8.2.3b, the BSL report no longer included GE_PORT type in the report.		

Condition:	Happens on extension platforms such as BR7840 running FOS8.2.3b.

16.3 Closed with Code Changes in 8.2.3b

Defect ID:	FOS-649549		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.0	**Technology:**	User Accounts & Passwords
Symptom:	Enable/disable root account using an AD account fails with error message: Cannot manage the target account due to conflicting AD permissions.		
Condition:	When using AD accounts to make changes.		
Workaround:	Perform the task via the default “admin” account		

Defect ID:	FOS-651997		
Technical Severity:	High	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.0.2c	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	One or more XTUN-1008 RASLOGs followed by tunnel down notifications at the peer switch.		
Condition:	Server with NPIV connections to fabric is frequently logging in and out of the fabric and issuing PLOGIs/PRLIs to devices over an FCIP Tunnel. Each PLOGI/PRLI has a new SID as the NPIV PID normally changes at each fabric login.		

Defect ID:	FOS-658218		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring

Reported In Release:	FOS7.4.1e1	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	Switch shows the wrong ip addresses in the login information log		
Condition:	SEC-1203 messages may show wrong IP during user login. No other functional impact.		

Defect ID:	FOS-800722		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.2	**Technology:**	Access Gateway
Symptom:	F-ports can end up in G-port or other inconsistent state.		
Condition:	After reboot or switchenable, F-ports and N-ports come online at the same time.		
Workaround:	Manually persistently disable all F-ports before reboot or switchenable. After reboot or switchenable, manually persistently enable the F-ports.		

Defect ID:	FOS-821089		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.0.1	**Technology:**	ISL - Inter-Switch Linking
Symptom:	Switch ports experience immediate hard fault or busy buffer stuck status which leads to a hard fault and possible switch fault of all ports.		
Condition:	Frequent plug/unplug of user port cables or a bad link causes physical errors that lead to port hard faults and/or credit loss.		
Workaround:	Do not plug/unplug links too frequently.		
Recovery:	Clean the link errors and bounce the ports with portdisable/portenable.		

Defect ID:	FOS-825815

Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS9.0.1	**Technology:**	FCIP
Symptom:	Kernel panic in DP during fcippathtest		
Condition:	This is a very rare occurrence that happens during diagnostic image bootup in DP upon execution of fcippathtest		

Defect ID:	FOS-827821		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.2a	**Technology:**	Optics
Symptom:	Device has login issue with certain optics types.		
Condition:	Enhance code to be more tolerant to RX LOS signals from optics.		

Defect ID:	FOS-830052		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1c	**Technology:**	CLI
Symptom:	Port initialization interop issues with a certain SFP, when connecting to a specific 3rd party device. This may result in some ports showing errors and some going into no_sync, port_Flt state.		
Condition:	This is seen with specific vendor SFP and is resolved via a new CLI "sfpprogram" enhancement to adjust port optics setting for interop. The new CLI syntax is as follows: sfpprogram port|port-range		

Defect ID:	FOS-830310		
Technical Severity:	High	**Probability:**	Medium

Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS9.0.0b	**Technology:**	CLI
Symptom:	Firmwaredownload fails with a generic error-message: "Firmwaredownload sanity check failed. Please contact the service provider if the issue persists."		
Condition:	This is seen in an environment with DNS configured, after the backend IP address between CPs on director are removed during firmwaredownload; Consequently ipaddress cannot be resolved and firmwaredownload timed out.		
Workaround:	'firmwaredownload -s' on both CPs.		

Defect ID:	FOS-831592		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	3rd party applications cannot collect performance information.		
Condition:	This is seen as a result of switch Boot time not being consistent with queries from SNMP on FOS8.2.3 and later and 9.0.1 and later. Applications relying on boot time to do calculations may get unexpected results.		

Defect ID:	FOS-831688		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2d	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	Various operations fail after the switch runs out of disk space.		
Condition:	This only happens with extension platforms. Netstat process on DP coredumps, filling DP's flash and in turn filling CP's flash during SupportSave operation.		

Workaround:	Remove the large number of core.netstat* files from /var/log/dpSlot0

Defect ID:	FOS-831875		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP application may lose connection to switch momentarily during snmp walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot.		
Condition:	This may occur when 3rd party applications or scripts perform mib walk on IPv6 address present in IP Address table (ipAddressTable) with partial indexes, such as "snmpwalk -v 3 -u snmpadmin1 10.155.22.131 1.3.6.1.2.1.4.34.1.2".		
Workaround:	Perform complete mib walk instead of querying for IPV6 entries alone.		
Recovery:	Normally snmpd will restart itself and connection will be restored shortly thereafter. However, if HA goes out of sync due to back to back snmpd restart failure during HA, a reboot is needed to recover.		

Defect ID:	FOS-832112		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2d	**Technology:**	FCIP
Symptom:	Switch panic after receiving invalid length frame.		
Condition:	This happens on extension platforms when the LACP/LLDP control frame has a length greater than 2112.		

Defect ID:	FOS-832434		
Technical Severity:	High	**Probability:**	High

Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a1	**Technology:**	CLI
Symptom:	After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch, with the following error: login: admin "Inconsistency de" - Note: traffic may be impacted too.		
Condition:	This impacts the Brocade 6548 switch only.		
Workaround:	Do not upgrade to FOS 8.2.3a on Brocade6548.		
Recovery:	No field recovery available but RMA switch.		

Defect ID:	FOS-832960		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.2d	**Technology:**	Trunking
Symptom:	Disruption on Access Gateways when F-port trunks change trunk master.		
Condition:	With a F-port trunking group and 1 F -port with 127 NPIV logins, the trunking master port was disabled, and the new master port got disabled too.		
Recovery:	Reboot fabric switch connected to AG.		

Defect ID:	FOS-833133		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.3a1	**Technology:**	CLI
Symptom:	When doing firmwarecleaninstall, the following will be displayed on the console: INSTALL26: ERROR - Cannot get file - /sbin/create_release_file. Please verify the network is good and retry firmwarecleaninstall after reboot INSTALL26: install FAILED with 0 warnings. FirmwareCleaninstall failed, you can reboot to retry.		
Condition:	firmwarecleaninstall on Gen5 platform		

Defect ID:	FOS-833550		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS7.4.2c	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	CP may encounter kernel panic when the FCIP DP generates a large number of XTUN-1006 events per second.		
Condition:	During FC Egress timeouts from the FCIP DP on an FX8-24 blade, the current implementation does not limit the number of XTUN-1006 RASLOGs that can be generated per second. When a severe event occurs where many FCIP FC Tx Timeouts occur, the FCIP DP will generate enough XTUIN-1006 RASLOGs to consume all CP memory resulting in the kernel panic.		
Workaround:	Fix the device that is causing the FCIP TX timeouts.		

Defect ID:	FOS-833935		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.3a	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	Encountered Weblinker posting raslog RAS-1004 with VERIFY after run out of file descriptor.		
Condition:	This issue is seen on switches running FOS8.2.3a with LDAP configuration during LDAP login from the management application.		

Defect ID:	FOS-833940		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2d4	**Technology:**	SNMP - Simple Network Management Protocol

Symptom:	SNMP panic resulted in director out of HA sync
Condition:	After using a 3rd party monitoring tool which sends a SNMPGET request with an invalid Fibre Channel port index. This could happen with FOS8.2.3 or later, FOS9.0.1 or later, FOS7.4.2h or later and the following CCEs: v8.2.2d4, v8.2.2c6, v8.2.1e1, v8.2.1c5.

Defect ID:	FOS-834163		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2d4	**Technology:**	FCIP
Symptom:	Extension tunnel on 7810, 7840 or SX6 blade will not come online in a NAT (Network Address Translation) enabled WAN environment.		
Condition:	When an extension circuit is configured to run over a WAN path that utilizes NAT, the circuit will not establish.		

Defect ID:	FOS-834621		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS9.1.0	**Technology:**	FCIP
Symptom:	eHCL sequence encounters fatal FICON FD error, which results in VE recovery.		
Condition:	This occurs when performing eHCL sequence over FCIP extended paths with FICON Emulation enabled on the tunnel(s) when there is active FICON IO.		

Defect ID:	FOS-834628		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2c6	**Technology:**	Extended Fabrics

Symptom:	User cannot create a tunnel after removing it.
Condition:	If LAN connections being extended to site A are in the process of getting established, and at the same time VE to another site B goes down, there is a small timing window in the LAN connection state machine handling, which can bring the LAN connection to a stuck state and it may never get cleaned up. In such cases, deletion of VE (under which LAN connections are not cleaned up) will not complete until the switch is rebooted.

Defect ID:	FOS-834868		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a	**Technology:**	Firmware upload/download
Symptom:	firmwareactivation CLI fails with SULB-1043, after staging a firmware upgrade/downgrade: 2021/09/22-14:58:50:367354, [SULB-1043], 76469/35239, SLOT 1 | CHASSIS, INFO, , Firmwareactivate command failed.		
Condition:	This results from a race condition that may be seen intermittently on an X6 chassis, if/when the firmwareactivate CLI context process falls behind the HA context process. The fix is only effective for future upgrades. This issue can still occur when upgrading "from FOS versions" that do not have this fix i.e. regardless of fix being in the target FOS version.		
Recovery:			

Defect ID:	FOS-834912		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.1.0	**Technology:**	Fibre Channel Services
Symptom:	SANnav reports error: "Registration for telemetry profile 'xxx' has failed and Switch panic after cald termination.		
Condition:	When schema server connection is unstable.		

Defect ID:	FOS-834918		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2d1	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	sfpshow CLI displays all zeros for txp, rxp etc smart data, and it triggers MAPs alert event.		
Condition:	It's mostly seen after a device offline/online.		
Recovery:	sfpshow <port> -f		

Defect ID:	FOS-835154		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.2d	**Technology:**	Name Server / Zoning
Symptom:	Dual CP reboot following some zoning changes performed via HTTP.		
Condition:	Panic occurs when multiple switches are performing configuration changes by webtools at the same time. This issue is more likely when one of the configuration changes fails.		

Defect ID:	FOS-835352		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2d3	**Technology:**	FCIP
Symptom:	Customer experienced temporary traffic outage due to tunnel bounce.		
Condition:	The outage happened due to DP reset recovery for a Datapath FPGA error. Enhanced code to gather more debug info for this situation.		

Defect ID:	FOS-835508

Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.3a	**Technology:**	ISL - Inter-Switch Linking
Symptom:	Switch panics while processing stale LISL entries.		
Condition:	This is caused as a result of stale LISL ports carried over from FOS v7.4.x / FOS v8.0.x release		

Defect ID:	FOS-835586		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a	**Technology:**	SNMPv2, SNMPv3 & MIBs
Symptom:	SNMP consumes more CPU cycles, resulting in MAPS alerts.		
Condition:	This issue occurs on platform where there are no GigE ports.		

Defect ID:	FOS-835791		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a	**Technology:**	Platform Services
Symptom:	Individual ports, that were previously disabled, are enabled while running CLI command switchcfgpersistentenable		
Condition:	This is seen with CLI command switchcfgpersistentenable when the switch persistent state is already enabled and the switch is already online.		
Recovery:	Re-disable the enabled ports.		

Defect ID:	FOS-836031		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management

Reported In Release:	FOS8.2.3a	**Technology:**	Fibre Channel Services
Symptom:	Switch panic after FDMI daemon terminated.		
Condition:	FDMI terminated after memory overrun during GPAT processing. This release addressed some port attribute length issues and also added enhancements to address and fix corruption around port attribute queries.		

Defect ID:	FOS-836043		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2b	**Technology:**	CLI
Symptom:	DCX8510 returning chassis S/N when being queried for brocade-chassis info via REST, when WWN 1 S/N was previously returned and used for entitlement.		
Condition:	When REST URL brocade-chassis/chassis URL is being used.		
Workaround:	Use CLI chassisshow to get WWN 1 serial number, or upgrade to a FOS version with fix and use the new leaf "entitlement-serial-number" via REST.		

Defect ID:	FOS-836219		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1c	**Technology:**	Optics
Symptom:	CLI "sfpshow -all" did not display complete output and the polling of smart SFP data stopped. It reported an very old "Last poll time:"		
Condition:	When SFP is plugged into a disabled port or SFP on disabled port is reseated.		
Workaround:	Run sfpshow -f to reactive smart data polling.		

Defect ID:	FOS-836265

Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3a	**Technology:**	Fibre Channel Services
Symptom:	During code upgrade from FOS v8.2.1x to FOS v8.2.3x, FOS cannot completely be brought up due to cald core dumps. User observes the switch hanging.		
Condition:	Issue is seen when ESRS is configured and call home alert is triggered before cald is initialized completely.		
Workaround:	Issue won't be seen without ESRS configuration. Users can bring up the switch by removing these "cal.esrs" entries from the configuration file.		

16.4 Closed with Code Changes in 8.2.3a1

Defect ID:	FOS-830052		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1c	**Technology:**	CLI
Symptom:	Port initialization interop issues with a certain SFP, when connecting to a specific 3rd device. This may result in some ports showing errors and some going into no_sync, port_Flt state.		
Condition:	This is seen with specific vendor SFP and resolved via a new CLI "sfpprogram" enhancement to adjust port optics setting for interop. The new CLI syntax is as follows: sfpprogram port|port-range		

Defect ID:	FOS-831875		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3	**Technology:**	SNMP - Simple Network

			Management Protocol
Symptom:	SNMP application may lose connection to switch momentarily during snmp walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot.		
Condition:	This may occur when 3rd party applications or scripts perform mib walk on IPv6 address present in IP Address table (ipAddressTable) with partial indexes, such as "snmpwalk -v 3 -u snmpadmin1 10.155.22.131 1.3.6.1.2.1.4.34.1.2".		
Workaround:	Perform complete mib walk instead of querying for IPV6 entries alone.		
Recovery:	Normally snmpd will restart itself and connection will be restored shortly thereafter. However, if HA goes out of sync due to back to back snmpd restart failure during HA, a reboot is needed to recover.		

Defect ID:	FOS-832434		
Technical Severity:	High	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	None	**Technology:**	CLI
Symptom:	After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch. Error shown as below: login: admin Inconsistency de Note: traffic may be impacted too.		
Condition:	This impacts the Brocade 6548 switch only.		
Workaround:	Do not upgrade to FOS 8.2.3a on Brocade6548.		
Recovery:	Swap partition from boot-prom to boot up from the alternate partition.		

16.5 Closed with Code Changes in 8.2.3a

Defect ID:	FOS-807030		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management

Reported In Release:	FOS8.2.1	**Technology:**	Platform Services
Symptom:	Performing vulnerability scans (Qualys) leads to high CPU load and Multiple config and secnotify processes are showing as consuming all memory.		
Condition:	This is encountered when vulnerability scans are being performed		

Defect ID:	FOS-818045		
Technical Severity:	Low	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.0	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Switch is flooded with messages, "attempts to send message type (1) to invalid dest (NSMIPC:0/0)", without any functional impact to switch.		
Condition:	This benign message occurs when performing SNMP IF.mib walk on platforms without Gige ports.		

Defect ID:	FOS-820640		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.0	**Technology:**	IPv6 Addressing
Symptom:	Flash usage exceeds 90% resulting in a switch panic.		
Condition:	Conditional race condition when user disabled dhcpv6, but dhcpv6 timer is still running which performs connection clean up by killing existing connection process. A code error passes an invalid parameter to the kill command when the dhcpv6 connection is non-existent. This resulting usage message from the failed kill command keeps growing the log file /etc/ipadmd_log.txt and depletes the available CF space.		
Recovery:	Cleanup the large log file.		

Defect ID:	FOS-820794

Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.2	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Switch remains in “MAPS Marginal state”, and cannot be cleared.		
Condition:	This occurs following a transient Power failure on any platform that has PSU FRUs with integrated / embedded FAN.		
Workaround:	Hareboot		
Defect ID:	FOS-820872		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.0.1	**Technology:**	BB Credits
Symptom:	Periodic Cx-1014 "frame loss" raslog messages may be logged without any traffic impact. Additionally, a link reset follows each frame loss detected occurrence.		
Condition:	This is encountered under following conditions: 1. A long distance Eport is configured with a distance over 255Km, and remote side is a 32G/64G platform, or 2. An F-port is configured with 8 or more credits on a 32G/64G platform.		
Workaround:	Disable the credit recovery or configure the HBA CR (bb_sc_n) number to less than 8.		

Defect ID:	FOS-822511		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS9.0.0	**Technology:**	Security Policies
Symptom:	After replacing MAC value in seccryptocfg, SSH and nmap show the value is not actually applied to one of the two CPs.		
Condition:	On executing “seccryptocfg --replace -type ssh -mac hmac-sha1 –force” on active CP, SSH MAC of Standby CP was still running on older SSH CP.		

Defect ID:	FOS-823675		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2b	**Technology:**	FEC - Forward Error Correction
Symptom:	On a 32G DWDM port, D_Port diagnostics fails on the spinfab throughput test and DWDM line flips fail.		
Condition:	This is specific to a 3rd party vendor 32G DWDM.		

Defect ID:	FOS-825546		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS9.0.1	**Technology:**	Extended Fabrics
Symptom:	SX6 DP Panic causing IO Failures		
Condition:	In a timing window during HCL or during error recovery sequences when a tcp connection is going away on WAN interfaces, invalid pointer could be accessed.		

Defect ID:	FOS-826088		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS9.0.1	**Technology:**	CLI
Symptom:	Switch paniced on long spinfab run - "ASSERT - Failed expression: VALID_PTR(ctl)"		
Condition:	Run spinfab for long duration.		

Defect ID:	FOS-826243		
Technical Severity:	Medium	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1e	**Technology:**	Rate Limiting and Shaping
Symptom:	The REST peak counters for fibrechannel-statistics seen as zero despite traffic flowing.		
Condition:	This is encountered when collecting port stats with REST API.		

Defect ID:	FOS-826244		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2c	**Technology:**	CLI - Command Line Interface
Symptom:	"sfpshow 5/31 -f -link" does not return correct information .		
Condition:	On a NPIV port, and attached device is RDP capable, CLI " sfpshow -f link" will not give the correct peer port gbic information.		

Defect ID:	FOS-826780		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.2d	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Add fence and decommission actions for the monitoring items TXP and RXP in the MAPS policy.		
Condition:	This enhancement will eliminate link instability due to SFP's Power fluctuations.		

Defect ID:	FOS-826987		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring

Reported In Release:	FOS8.2.2c	**Technology:**	Port Mirroring
Symptom:	'filterportshow' output is incomplete and switch panic with console output, "BUG: Bad page map in process supportsave".		
Condition:	Mirror flows are configured, either by the customer or due to AE-port, when there are high number of cam entries. Then run the 'portfiltershow' command either manually or in supportsave to trigger this.		

Defect ID:	FOS-827021		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.0.1a	**Technology:**	FC-FC routing
Symptom:	In an EX-port trunk. frames routed to the slave port are dropped, result in LUN discovery issues after an edge fabric split and merge.		
Condition:	This is a corner case scenario occurring in specific topologies having trunked EX-Ports when they are in the process of getting disabled due to Fabric ID (FID) conflict, then re-enabled. If the EX-port trunk comes back onlline and uses a new PID for the master EX-port, this issue is observed.		

Defect ID:	FOS-827217		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.2d	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	Switch panic during tracedump.		
Condition:	Trace module memory is somehow corrupted. Any subsequent event that triggers a FFDC or a Supportsave on switch, could cuase the switch to panic.		

Recovery:	After panic, the switch is recovered without further action. With FOS8.2.3a, the panic is avoided and a raslog "KTRC-1006: Trace corruption found." can identify the event has occured.

Defect ID:	FOS-827719		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	CORE and FFDC are generated on newly active CP after a dual CP firmwaredownload.		
Condition:	This is a very rare occurrence triggered by a hard to reproduce timing issue hit when EM module cannot present the blade list information to snmp daemon in a timely manner when the newly downloaded CP takes over the active CP role.		

Defect ID:	FOS-827741		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2b	**Technology:**	Management Server
Symptom:	MAPs messages use old port labels.		
Condition:	When one changes portname of a port after the Fabric Vision license has expired or without a Fabric Vision license.		

Defect ID:	FOS-827821		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.2a	**Technology:**	Optics
Symptom:	Device has login issue with certain optics types.		

Condition:	Enhance code to be more tolerant to RX LOS signals from optics.

Defect ID:	FOS-827976		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.0b	**Technology:**	High Availability
Symptom:	cold boot after ONMd crash when standby becomes active during hafailover process.		
Condition:	This is a rare occurrence resulting in corrupted timers following an Hafailover.		
Recovery:	The switch should be recovered when the switch comes back up after the crash.		

Defect ID:	FOS-828208		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1a	**Technology:**	Hardware Monitoring
Symptom:	Webtools hardware view does not show the Led status correctly for ports 50, 51 and 117 .		
Condition:	This issue is observed only for Brocade G630 switch and isolated to webtools only. CLI correctly shows the ports as online.		

Defect ID:	FOS-828373		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.2d	**Technology:**	HTTP/HTTPS
Symptom:	seccertmgmt_create.py reports 400 as "client-error-code".		

Condition:	The issue is seen while generating the certs using secertmngt via pyfos and REST.

Defect ID:	FOS-828392		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2c	**Technology:**	AAA
Symptom:	Port Optics is not visible in Sannav with error: Fail to get SFP details.		
Condition:	It fails for remote users such as LDAP/RADIUS/TACACS.		

Defect ID:	FOS-828899		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	DP Panic after upgrading to FOS8.2.1 through FOS8.2.2d while running FICON XRC traffic over XRC Emulation enabled FCIP Tunnel.		
Condition:	When processing back to back Command Retry Status and Device End status frames for an XRC Read Record Set chain.		

Defect ID:	FOS-829310		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	FICON
Reported In Release:	FOS8.2.3	**Technology:**	FICON emulation
Symptom:	FICN-1062 or FICN-1063 with LastStates=0x005E005E0068 indicating that there were FICON Abort sequences processed on the emulated tunnel.		

Condition:	When recovering FICON control units over a FICON emulation enabled FCIP Tunnel with FICON Dynamic Routing (EBR) mode enabled.

Defect ID:	FOS-829423		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2d	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	FCIP DP Panic and DP Reset after switching an FCIP Circuit from wantool testing state back to active FCIP Circuit		
Condition:	Run WAN Tool and return to normal state over an FCIP Circuit		

Defect ID:	FOS-829441		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2d	**Technology:**	WAN Performance Analysis Tools
Symptom:	"XTUN-1001 : memory allocation error" messages in RASLOG after using FCIP SLA or manual WTOOL functionality.		
Condition:	DRAM2 memory allocation failures after WTOOL DRAM2 leak gets too severe. Leak occurs during WTOOL session deletion.		
Workaround:	reboot.		
Recovery:	Upgrade to code with WTOOL DRAM2 leak fix.		

Defect ID:	FOS-829454		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.0b	**Technology:**	CLI - Command Line Interface
Symptom:	Port blade comes up as faulty after diagnostic run.		

Condition:	This is seen when the "runs" parameter of the "systemverification" CLI command is set to value 4 or higher.

Defect ID:	FOS-829537		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1d	**Technology:**	Access Gateway
Symptom:	Following an hareboot, the agautomapbalance configuration is not the same as it was before the hareboot.		
Condition:	agautomapbalance setting is changed when no other commit of configuration DB is done before hareboot.		

Defect ID:	FOS-829594		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	FICON
Reported In Release:	FOS9.0.1b	**Technology:**	FICON
Symptom:	Issuing a switchenable when the switch is already enabled may lead to I/O disruption		
Condition:	Running switchenable when the switch is already enabled and has LISLs.		
Workaround:	Check if the switch is enabled first before running switchenable.		
Recovery:	The bounced LISL comes back up on its own.		

Defect ID:	FOS-829779		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.3	**Technology:**	Management Server

Symptom:	SANNAV fails to generate switch supportsave on switches running FOS v8.2.2 and above.
Condition:	When SANnav initially sets up to use non-default port, and then later changed to use the default port of 22 for scp/sftp data transfer, switch continues to send data through non-default port and is rejected by SCP/SFTP server. This defect does not apply to FOS v9.x.
Workaround:	Configure SCP/SFTP server to listen on non-default port. Alternatively please gather supportsave through CLI until FOS code is upgraded.
Recovery:	A hafailover/hareboot can recover from this condition.

Defect ID:	FOS-830884		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2	**Technology:**	Web Tools
Symptom:	WebTool "Switch Administration -> Extended Fabric" tab are missing slots for X6 directors.		
Condition:	Using Web Toool, slots 6 and 7 are not displayed for X6-8 and slots 4 and 5 are not disapled for X6-4 on Extended Fabric tab.		

16.6 Closed with Code Changes in 8.2.3

Defect ID:	FOS-800300		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	CLI - Command Line Interface
Symptom:	Route is invalid on G630 E-ports.		
Condition:	After running offline diag tests on G630, route may fail and frames may drop.		
Workaround:	Reboot the G630 after running offline Diag test (Plb, turboramtest , portledtest and systemverification).		
Recovery:	Reboot the switch.		

Defect ID:	FOS-801436		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2a	**Technology:**	RBAC
Symptom:	Customer encounters SNMP query failure on VF.		
Condition:	This occurs when the user is mapped to a custom role with RBAC class of admin.		

Defect ID:	FOS-803493		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.0.2b	**Technology:**	Ethernet Interface
Symptom:	X6 eth0 reverting to 10/half when ethif is used to configure speed/duplex settings while network connection is removed		
Condition:	Configure eth0 when Ethernet cable is disconnected.		

Defect ID:	FOS-803567		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.2	**Technology:**	Hardware Monitoring
Symptom:	CLI sfpshow has incorrect SFP low tx values.		
Condition:	This is occasionally seen for QSFPs.		

Defect ID:	FOS-804873		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS

Reported In Release:	FOS8.2.1	**Technology:**	Audit Log
Symptom:	Audit log only displays the last command issued.		
Condition:	The failure shows when the auditlog storage file is corrupted for unknown reason.		
Workaround:	Run "auditdump -c" to reset the auditlog storage file,		

Defect ID:	FOS-804971		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.1.2a	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	Switches showing MAPS-1003 raslog with 0mvolt messages on port with SFP and QSFP.		
Condition:	QSFP values(volt,temp,rx power,current) is read as zero in regular polling. Added retry logic to improve data sampling.		
Defect ID:	FOS-805305		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	D-Port - Diagnostic Port
Symptom:	D-Port test fails with Protocol Error on switch end and on HBA, EL failed despite the overall result states Passed		
Condition:	D-port test gets failed/ stuck in IN_PROGRESS when the test is executed on the QSFP links connected to GEN5 HBAs.		

Defect ID:	FOS-805457		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS7.4.2c	**Technology:**	Frame Redirection

Symptom:	Silent frame drops may be encountered on Brocade 6520.
Condition:	This occurred because the BE link DID check bit was set in the past, which led to frame drops over that particular BE link.

Defect ID:	FOS-806463		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.2b	**Technology:**	Port bring up
Symptom:	Following HA failover some ports appear to encounter ASIC stats errors which causes these ports to be fenced if MAPS is configured to fence ports for ITW.		
Condition:	The low level asic stats errors are not caused by the HA failover action and appear to be from a prior uninitialized condition.		
Workaround:	Clear the stats before HA failover.		
Recovery:	After the port is fenced, bring it back online again.		

Defect ID:	FOS-806547		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Distance
Reported In Release:	FOS8.2.0b	**Technology:**	Extended Fabrics
Symptom:	The ISL link between two G620 switches fails to recover and goes to "HRD_FLT" state.		
Condition:	This is seen after repeated cable-pull tests. Issue is also reported on F-port.		

Defect ID:	FOS-807056		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS

Reported In Release:	FOS8.2.1	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	Test email is not sent out by switch.		
Condition:	During hafailover, domain name is not getting synced to sendmail file, email will not be send.		

Defect ID:	FOS-807249		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1a	**Technology:**	Ethernet Interface
Symptom:	Switches lost management IP config after reboot.		
Condition:	It happens when the gateway address is set to 12 full digits.		
Workaround:	Avoid reboot switch if gateway address is set with 12 full digits until upgrade. Or use less than 12 digits gateway address		
Recovery:	After each reboot customer has to login via serial cable to make any changes.		

Defect ID:	FOS-807784		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.0.2	**Technology:**	CLI
Symptom:	portloopbacktest is unable to detect CRC error.		
Condition:	When there is CRC errors on link		

Defect ID:	FOS-808426		
Technical Severity:	Medium	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1a	**Technology:**	Bottleneck Detection (legacy)
Symptom:	CLI "mapsdb --congestion" shows an event but "mapsdb --congestion -freq" doesn't show it.		
Condition:	MAPS had wrong port stats about congestion details leading to this mapsdb show congestion/frequency inconsistencies.		

Defect ID:	FOS-808461		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.0	**Technology:**	CLI - Command Line Interface
Symptom:	Switch panic during diagnostics test.		
Condition:	Issue was observed during spinfab or portloopback traffic test. Especially when the test was abort with a control-c.		

Defect ID:	FOS-808514		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1a	**Technology:**	Management Server
Symptom:	After a host behind an NPIV device reboots, it is unable to discover any of its LSAN devices.		
Condition:	Under a rare condition, intercommunication packets between name server were dropped.		
Recovery:	Perform a hafailover to recover name server communication.		

Defect ID:	FOS-808560		
Technical Severity:	High	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS9.0.0	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	When a longer FQHN is used for TACACS+ authentication, local accounts as well as AAA accounts are not accessible.		
Condition:	Only when tacacs+ is configured		

Defect ID:	FOS-809213		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.0.2c	**Technology:**	Configuration Fundamentals
Symptom:	Switch panics after various daemons, such as fcpd, tsd, webd, terminate while accessing configuration database resource key.		
Condition:	This is mostly observed on Gen6 fix-port switches such as G620; However, it has been seen on BR7840 and directors. Configuration database resource key is cached in shared memory and frequently accessed by daemons. Sometimes, the shared memory used by daemon is no longer valid while configDB on permanent storage is still intact.		
Recovery:	Switch recovers after panic without further action.		

Defect ID:	FOS-809425		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.1.0	**Technology:**	SSH - Secure Shell
Symptom:	When a crypto template is applied, the existing SSHd session is not terminated.		
Condition:	After applying a SSH crypto template , the existing session remains open.		
Workaround:	The --replace option handles the situation correctly		

Defect ID:	FOS-810413		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Access Gateway
Symptom:	Missing N-port info from "ag --show" after toggle N-ports.		
Condition:	After toggling N-ports that connect to Gen5 and Gen4p , "ag --show" has missing N-port info "Attached_Switch", "Switch F-port" and "IP_Addr". This is seen on FOS v8.x and later.		

Defect ID:	FOS-810630		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1b	**Technology:**	Fibre Channel Services
Symptom:	Users may encounter FDMI daemon termination.		
Condition:	This is seen when FDMI attempts to deallocate the buffers used to get the HBA/Port entries. The dynamically allocated block attempted to be freed appears to be invalid due to memory overrun.		

Defect ID:	FOS-811237		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS7.0.0d	**Technology:**	Name Server / Zoning
Symptom:	Zone daemon panic observed during zone change.		
Condition:	When there is a transaction already open in a switch (ex: via CLI) and another transaction starts (distribution via ACA, SFC, UFC, RCA through WT/BNA) in a remote switch in the same fabric simultaneously. This is a timing issue when a customer creates multiple zoning transactions on different switches at the same time.		
Workaround:	Use the cfgtransshow cli command to confirm there are no outstanding zoning transactions before initiating a new one.		

Recovery:	The switch recovers after the ASSERT.

Defect ID:	FOS-811459		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.0.2d	**Technology:**	supportShow
Symptom:	System may encounter emd termination resulting in failover to Standby CP.		
Condition:	This is seen during supportsave collection, possibly due to memory corruption		

Defect ID:	FOS-811539		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.0.0	**Technology:**	BB Credits
Symptom:	POST on /rest/operations/device-management/ returns a PLOGI ELS reject error message. Credit field in portloginshow output may be large number. End devices may suddenly logout after hareboot/hafailover.		
Condition:	Issue happens when perform HA failover / HA reboot in a logical switch without port index of zero.		
Workaround:	Move the device to a logical switch where port index zero exists.		
Recovery:	Bounce the port.		

Defect ID:	FOS-811952		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.1.2d	**Technology:**	Component

Symptom:	Experience silent reboot (reboot reason: reset) or switch hung for hours/days.
Condition:	Running script with nested or concatenated CLI commands over 512 bytes long.
Workaround:	Allow 5 seconds of idle time between commands and keep CLI length under 512 bytes.

Defect ID:	FOS-812267		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1	**Technology:**	Hardware Monitoring
Symptom:	A good replacement blade cannot come up with raslog [EM-1134] rc=20074: 2019/11/19-11:28:33:895421, [EM-1134], 95966/2420, SLOT 2 | FFDC | CHASSIS, ERROR,, Slot 7 set to faulty, rc=20074., OID:0x43700000, em_board_lib.c, line: 1944, comp:emd, ltime:2019/11/19-11:28:33:895302 And after CLI "slotpoweron" bring back the blade, it is powered off again after active CP reboot,		

Condition:	After a blade is intentionally powered down due to PCI errors by FOS, or by a user issued slotpersistentpoweroff, while running FOS8. 1.0 or earlier, a replacement blade does not power up, or if it is powered back up via "slotpoweron" CLI command then it is powered down again after CP reboot.
Recovery:	1. Make sure that a good replacement blade is inserted and power it on via the "slotpoweron" CLI command. 2. Perform an hafailover; wait for hasync 3. Perform another hafailover Note: please use slotpoweron to recover, and do not use slotcfgpersistent --poweron to recover the blade.

Defect ID:	FOS-812536		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1b	**Technology:**	SNMP - Simple Network

			Management Protocol
Symptom:	SNMP community strings with basic SNMPv1 queries are not recognized.		
Condition:	A timing condition in code caused snmpconfig commands fail leading to database inconsistency and snmp queries become unresponsive		
Recovery:	Need to restart snmpd or switch reboot		
Defect ID:	FOS-812556		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.1b	**Technology:**	HTTP/HTTPS
Symptom:	Weblinker cannot restart with continuous messages; "system is not ready for HA/LS CLI cmd".		
Condition:	After a configuration change such as "seccertmgmt generate -cert https -years 20 -f".		

Defect ID:	FOS-812883		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS7.4.2c	**Technology:**	Frame Monitoring
Symptom:	Customer may encounter frame drops corresponding to specific SCSI task management commands.		
Condition:	It happens when multiple end devices connected to the same 16G ASIC going through an error recovery which floods the ASIC with PLOGI/ADISC.		

Defect ID:	FOS-812889		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension

Reported In Release:	FOS9.0.0	**Technology:**	Extended Fabrics
Symptom:	SX6 blade is not powered-on, when initializing the blade, after EM_INCONSISTENT failure during HA failover.		
Condition:	During hafailover after SX6 blade DP soft failure.		

Defect ID:	FOS-812985		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.1.2j	**Technology:**	Component
Symptom:	Kernel or user daemon panic caused by trace module corruption.		
Condition:	Trace module is corrupted and subsequently when user daemon or kernel attempts to log a trace, switch may experience a panic.		
Recovery:	Switch recovers automatically after the panic without requiring further action.		

Defect ID:	FOS-813157		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1b	**Technology:**	Management GUI
Symptom:	Some port stats are missing.		
Condition:	Ports with USER-PORT greater than the number of physical ports present were missed during data collection. ICL ports can have a user port number greater than max_phy_port. However the total physical ports will never exceed max_phy_port.		

Defect ID:	FOS-813299		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring

Reported In Release:	FOS8.2.1c	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	After running statsclear on default switch, 'Current' counts of '4 History Data' section of maps database for Base Switch is cleared.		
Condition:	This issue is reproducible on Port-3/0 only after running statsclear CLI.		

Defect ID:	FOS-813523		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.0.1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	BR7840 or SX6 FCIP Tunnel failure or disable can result in DP reset		
Condition:	Small timing window when FC frames can be received on the FCIP tunnel after the tunnel is reported as going offline. It is occasionally observed on FOS v8.x.		

Defect ID:	FOS-813525		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.0	**Technology:**	Configuration Fundamentals
Symptom:	Fibre channel port statistics counters report large values such as "4294967295" after statistics reset.		
Condition:	Counters become invalid after stats reset or during simultaneous data gathering through CLI and REST API.		

Defect ID:	FOS-813692		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.2j	**Technology:**	Port bring up

Symptom:	Lot of I/O failures and traffic disruption reported after performing HA failover on Gen6 chassis-based switches.
Condition:	Port blade and/or core blade slot power cycles, followed by HA failover.
Recovery:	Core blade power off and power on recover from this state.

Defect ID:	FOS-813777		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.0.0	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP OIDs swConnUnitPortTxRate and swConnUnitPortRxRate always show zero values when querying the switch in AG-mode.		
Condition:	This is seen with switch running FOS 8.x and above and is in AG mode.		

Defect ID:	FOS-813796		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.0.1	**Technology:**	FCIP Tunnel Management
Symptom:	The user will observe the Tunnel bounce when changing circuit bandwidth.		
Condition:	This stems from a bug during PMTU busy retry and applies to FOS 8.x and above.		

Defect ID:	FOS-814082		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension

Reported In Release:	FOS8.2.1	**Technology:**	Extended Fabrics
Symptom:	Switch panic due to esmd termination		
Condition:	This occurs due to a timing issue when CLI debug command is run early in the switch initialization phase. This applies to FOS 8.x and above.		

Defect ID:	FOS-814152		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.1.2	**Technology:**	Frame Monitoring
Symptom:	Customer enabled framelog to capture unroutables , but not all frame drops are captured in the framelog.		
Condition:	This issue is seen when the frame drop is less than 20 per second on the port where the drop is being observed		

Defect ID:	FOS-814430		
Technical Severity:	Low	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.1	**Technology:**	supportShow
Symptom:	Diag related logs are not present in SupportSave.		
Condition:	This applies to Brocade Switch BR7810 running FOS 8.x and above.		

Defect ID:	FOS-814484		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.1c	**Technology:**	User Accounts & Passwords

Symptom:	Creating a user account with an uppercase password causes the login to fail.
Condition:	Create user account in uppercase as below: >userconfig --add USERID -r admin -d "Default Admin" -p PASSW0RD Account USERID has been successfully added. login: USERID password: (PASSW0RD) LOGIN INCORRECT
Workaround:	Lower case password works

Defect ID:	FOS-814782		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1c	**Technology:**	CLI - Command Line Interface
Symptom:	Firmwarecheck failure on ASC-G certificate file.		
Condition:	There is no functional impact to majority of customers with default switch configurations. Switch may be forced into a reboot loop if *all* the following conditions are met: 1. User should have automatic 'firmwarecheck' enabled on the switch ("firmwarecheck --enable") 2. User should be using ASC-G 3. User should have imported enterprise CA certificate for the ASC-G. In the above state, if and when the switch is rebooted it will result in rolling reboot due to 'firmwarecheck' failure. This applies to FOS8.2.1c and FOS8.2.2.		
Defect ID:	FOS-814807		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS9.0.0	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	SX6 AP blade fault occurs after internal backend port is disabled or a disruptive failover even though it reports HA-IN-SYNC.		
Condition:	When the active CP has a non-default blade mode (either VE-MODE set to 20VE, or APP-MODE set to hybrid) and the standby CP is installed for the first time, or netinstalled, the standby CP will have the wrong app-mode.		
Recovery:	Reboot the standby CP before any failover attempts are made.		

Defect ID:	FOS-815116		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.0	**Technology:**	Component
Symptom:	The BR6520 switch gets into a rolling reboot loop and needs a manual intervention to recover.		
Condition:	When a bad asic access caused the PCI bus to hang. This impacts BR6520 switches only.		
Recovery:	Reboot switch to recovery		
Defect ID:	FOS-815150		
Technical Severity:	Low	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	Access Gateway
Symptom:	AG default mapping is incorrectly set for Brocade 6547 switch.		
Condition:	This is seen when enabling AG mode, the F-port-to-N-port mapping is incorrect.		
Recovery:	Manually unmap the wrong ports from N-port 0 and then map the correct ports to N-port 0. Also, the unmapped ports may need to be converted to N-ports (portcfgnport) and have mapping applied to them.		

Defect ID:	FOS-815152		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.2	**Technology:**	CLI
Symptom:	During firmwaredownload, the error message is not properly worded.		
Condition:	Perform CLI firmwaredownload on a switch with ethernet management port configured in half duplex mode.		
Workaround:	Configure switch management port to Full Duplex mode. Half duplex mode is not supported.		

Defect ID:	FOS-815189		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.1b	**Technology:**	Security Policies
Symptom:	Supportshow is incomplete due to "Permission denied" on /var/log directory.		
Condition:	Run supportshow with admin privilege.		

Defect ID:	FOS-815218		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.1.2a	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	FCIP DP panics		
Condition:	After aborts have been processed on a FICON Emulation enabled tunnel when end device re-used an exchange.		
Recovery:	It recovers after panic.		

Defect ID:	FOS-815265		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Fibre Channel Services
Symptom:	Observing RTWR error on fabric with DISL.		
Condition:	It happens after a cold boot or core blade slotpoweron. Routes for ICL ports are incorrect such that fabric services on different switches cannot communicate. This applies to FOS8.2.1 and above.		
Workaround:	Perform an hafailover on the chassis.		

Defect ID:	FOS-815327		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0b	**Technology:**	Inband Management
Symptom:	Switch panic observed after essd daemon access freed memory.		
Condition:	During high CPU time (for example, during lots of SNMP requests), inter-switch communication can be delayed and cause a daemon and/or switch crash.		
Workaround:	Try to reduce SNMP requests.		
Defect ID:	FOS-815352		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.1.2j	**Technology:**	Extended Fabrics
Symptom:	IPEX LAN TCP connection will report failed in the application.		
Condition:	When there is packet loss on the LAN with Jumbo frames enabled, the LAN TCP receive process may stall causing LAN TCP connections to timeout.		

Defect ID:	FOS-815828		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS7.4.2g	**Technology:**	SSH - Secure Shell
Symptom:	When changing templates and performing HA failover, the SSH config is not replicated to the standby CP.		
Condition:	This occurs on director class dual CP systems.		

Defect ID:	FOS-815835		
Technical Severity:	Medium	**Probability:**	Medium

Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1	**Technology:**	Name Server / Zoning
Symptom:	These non-intrusive misbehaviors observed on device enforcement: 1. Move a port from default switch to logical switch, original PID in the default switch still exists in the new logical switch. 2. Prohibit two local ports by PDCM in FICON environment. Routing is still allowed between the two ports.		
Condition:	This applies to FOS8.2.1 and later releases.		

Defect ID:	FOS-815880		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS8.2.1d	**Technology:**	Access Gateway
Symptom:	When the Access Gateway switch has a single connection to the director and porttrunkarea is set on the director, the Access Gateway switch does not report the Switch F-port number.		
Condition:	Access Gateway is connected to a Gen6 chassis in non-VF mode, N_Port information is missing the port index of the connecting fabric switch. This impacts FOS8.2.0 and later.		

Defect ID:	FOS-815893		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1c	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Logical group used in rule can be deleted due to inconsistent handling of letter case.		
Condition:	While deleting the map rule under active policy. Also while deleting rules with -force option.		

Workaround:	Use proper group names or actual group names that are not differentiated by case alone.

Defect ID:	FOS-816023		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.0.1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	FX8-24 with XRC Emulation Enabled, DP panic encountered.		
Condition:	This is seen when system reset occurs with active IO in FX8-24 FCIP configuration with FICON Emulation enabled for XRC traffic.		
Defect ID:	FOS-816025		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS8.2.1a	**Technology:**	NPIV - N-Port ID Virtualization
Symptom:	Standby CP encountering Out Of Memory (OOM) reboot on task esmd		
Condition:	Devices logging in and out of F-ports multiple times per second.		
Workaround:	Reduce the login/logout frequency of devices.		
Recovery:	Switch is recovered after OOM action.		

Defect ID:	FOS-816203		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.0b	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Trunk Rx per hour is reported as 100% with raslog MAPS-1004.		
Condition:	When there is trunk and the trunk's Rx is divided by single port's sample time instead of trunk's average sample time on all FOS8.x.		

Defect ID:	FOS-816251		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0	**Technology:**	NPIV - N-Port ID Virtualization
Symptom:	Traffic is being routed to the wrong ports.		
Condition:	It happens when connecting G610 AG switch to a future platform and more than 63 NPIV devices are connected.		

Defect ID:	FOS-816274		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Fibre Channel Services
Symptom:	When viewing the devicelogin --show output, fabric interconnect devices may not join the existing members of a group.		
Condition:	Specific third party devices connected to ports that have area 0xff in the Port Address.		
Workaround:	Move the connection to a port without 0xff area.		

Defect ID:	FOS-816300		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1c	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP-Get ipNetToMediaIfIndex returns "lo" on X6 and "chassis" on DCX8510. Both should return "eth0".		
Condition:	Issue will be seen upon querying ipNetToMediaIfIndex.		

Defect ID:	FOS-816655		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS9.0.0	**Technology:**	Virtual Fabrics
Symptom:	Switch panic during code upgrade.		
Condition:	This may occur if the user previously performed a switchdisable / switchenable, in quick succession without a time gap of minimum 5 minutes, on a base switch running pre-FOS8.1. This may result in stale LISL left on the switch, which triggers the switch panic during subsequent upgrade to FOS8.2.x .		
Workaround:	Provide a minimum time gap of 5 minutes between the last disruptive operations (e.g. switchdisable/switchenable).		

Defect ID:	FOS-816740		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1b	**Technology:**	ISL - Inter-Switch Linking
Symptom:	LISLs offline following upgrade from from FOS8.0.x to FOS8.1.x-->FOS8.2.x		
Condition:	This occurs due to stale lisl ports in code being carried over from FOS8.0.x FOS8.2.x		

Defect ID:	FOS-816787		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS9.0.0	**Technology:**	SSH - Secure Shell
Symptom:	SSH client and server advertises its version number.		
Condition:	OpenSSH version number of Brocade switches reported during nmap scan of SSH port		

Defect ID:	FOS-816973		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Historical graph values for TX/RX are all zeros. Real-time graph values are accurately displayed.		
Condition:	When displaying historical graph values for TX/RX, the historical display may show all zeros when monitoring on GEN 6 platforms. Happens only when monitoring for historical graph values (Real-Time graph values for TX/RX have no issue). Issue is only seen when monitoring from BNA 14.4.4 or BNA 14.4.5. Issue is not seen with older versions of BNA or with SANnav.		
Recovery:	Rarely seen on GEN 5 platforms, but will recover on next historical display request.		

Defect ID:	FOS-817144		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS9.0.0	**Technology:**	Port bring up
Symptom:	FCoE device does not login causes random storage disconnects.		
Condition:	When connected to a 3rd party switch, all LLDP TLV's are discarded on the port after a cold reboot of the active CP.		
Recovery:	Toggle fcoe mode.		

Defect ID:	FOS-817564		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2a	**Technology:**	Fibre Channel Services

Symptom:	Kernel Panics/cold recoveries encountered in core switches, following exchanges getting timed out.
Condition:	This is seen when an end device sends out-of-order mal-formed multi-frame Common Transport sequence destined for the Name Server that appears to be a single-frame sequence and a multi-frame sequence with the same sequence ID. Other Name Server destined frames are being received at the same time.
Workaround:	Disable the offending end devices.
Recovery:	The switch recovers after the cold boot.

Defect ID:	FOS-817671		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS9.0.0	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	Observed verify when enabling the D-port mode.		
Condition:	credit zero stats were not correct when port joins or leave trunk.		

Defect ID:	FOS-817829		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS8.2.1b	**Technology:**	Virtual Fabrics
Symptom:	Switch reboot after execute "lscfg --delete" command to deleting a logical switch.		
Condition:	A race condition happened while executing “lscfg –delete ” and “agshow” command at the same time. CLI agshow accessed memory just being freed by lscfg.		
Workaround:	Run “lscfg –delete ” and “agshow” commands two minutes apart.		

Defect ID:	FOS-817849		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.1c	**Technology:**	Equipment Status
Symptom:	Need to perform switch excess power check and shutdown for BR7840 and 6520.		
Condition:	This may happen under rare situation that may cause the board to draw excessive power		

Workaround:	A CRITICAL raslog EM-1229 is logged when the power consumption is detected to be within 20% limit of reaching the threshold for excessive power. The user is advised to power down the system and contact Brocade support to have the system replaced
Recovery:	In the event of that the EM-1229 raslog goes unheeded and the power drawn crosses the excessive power threshold then the system will log raslog EM-1230 and power off the system. The user must contact Brocade support to have the system replaced

Defect ID:	FOS-817875		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.1e	**Technology:**	supportShow
Symptom:	"Unable to handle kernel paging request" issue seen during SupportSave collection resulting in HA failover.		
Condition:	Under heavy cpu load, running supportsave or chipregdmp caused ASIC thread deadlock.		
Workaround:	Do not run parallel supportsave or asic related dump when system is under heavy load.		
Recovery:	Reboot the impacted switch.		

Defect ID:	FOS-817953		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1c	**Technology:**	Zoning
Symptom:	After making zone changes in the fabric, customer may encounter one or both of the following: 1. Defined zone configuration DB is removed, HA Sync is lost, and verify error seen on standby CP. 2. Fabric is segmented with reason "segment zone conflict" If the zone data base is not repaired before issuing a cfgEnable to activate the new zone definition, it can result in an impact to traffic.		

Condition:	This issue can be seen with FOS8.2.1, 8.2.1a, 8.2.1b, 8.2.1c,8.2.1d, 8.2.2, 8.2.2a or 8.2.2b. When a very specific 3rd party device sends the Get Active Zone Size (GAZA) / Get Zone Size (GZS) CT command with limited response size. Zone database is corrupted after processing these commands, and an extra semicolon is left at the end of the zone member list.
Workaround:	Avoid using "network fcp zone show" from the device, which triggers GAZS/GZS request to fabric.
Recovery:	If the defined zoning database was truncated but no zone commit operations were performed: Option 1: From another switch in the fabric that has not been corrupted with the extra semicolon, create a "dummy zone" and then perform a "cfgEnable" command on the effective cfgname to restore the zoning database across the fabric. Option 2: On the switch that has the added semicolon in the zone data base, perform an "haFailover" if it is a director or an "haReboot" if it is a fixed port switch. Option 3: Coldboot the switch with the bad zonset. If the bad zonset was pushed to the rest of the fabric, and the zoning data base is erased: Options presented in order of least disruptive to more disruptive: Option a: On a remote switch that has an empty defined zoning database issue an "haFailover" if it is a director or an "haReboot" if it is a fixed port switch. When complete, the zone database should be restored. Next, create a "dummy zone" and perform a "cfgEnable" command on the effective cfgname to restore the zoning database across the fabric. Option b: Issue an "haFailover" or "haReboot" on all directors and switches in the fabric respectively. Option c: Cold boot all switches in the fabric. Once zoning has been restored to all switches in the fabric, do not issue the "Network fcp zone show" command from the third party storage array or the failure could re-appear.

Defect ID:	FOS-817960		
Technical Severity:	Low	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1c	**Technology:**	CLI - Command Line Interface
Symptom:	For the configupload command, the -force flag when saving to the local file system does not work. It still prompts the user if they would like to overwrite the previous file.		
Condition:	This is encountered when attempting to force save the config to local file: configupload -force -local		

Defect ID:	FOS-818055		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1c	**Technology:**	High Availability
Symptom:	Brocade Gen6 Director switches may encounter one or both of the following occurrences: 1. Standby CP reports hasmd panic and active CP reports pdmd panic, leading to cold recovery. 2. User performs lscfg operation, which fails with raslog [PMGR-1006], 204690/5858, SLOT 1 | CHASSIS, WARNING, , Attempt to move port(s) -1 on slot -1 to switch failed.		
Condition:	This can only occur on X6-8 or X6-4 director switches after upgrading to FOS 8.2.0 or later versions from an earlier FOS version, and the PORTMAP table grows in size >= 1024. PORTMAP table size can only grow beyond 1024 characters after using the "lscfg" CLI command repeatedly moving ports between logical switches. The current PORTMAP table size can be calculated by using CLI command "configupload -vf | grep PORTMAP" and count the characters starting from "F" or "G" to the ending "]" character. X6-8 or X6-4 director switches shipped from the factory with 8.2.0 or higher FOS already installed will not be exposed to this issue unless they were downgraded to a version of FOS prior to v8.2.0 and then upgraded again to FOS 8.2.0 or later.		
Workaround:	Upgrading from a FOS version prior to v8.2.0 directly to FOS 8.2.2b or later will avoid this issue. If the switch was previously upgraded to a version of FOS 8.2.0 or higher prior to upgrading to FOS 8.2.2b, then the upgrade to FOS 8.2.2b alone will not repair the PORTMAP table.		
Recovery:	A non-disruptive process to repair the PORTMAP table can be performed, but requires ROOT access to issue the required command(s) to repair the PORTMAP table. Contact Brocade Support if the PORTMAP table is growing (GE or FC) near the 1024 size limit. The set of commands to repair the PORTMAP table can then be provided after examining a SupportSave from the switch. Alternatively, a disruptive recovery process can be followed for users that do not have ROOT access to their switch: 1. configupload -vf 2. Manually modify the uploaded VF config file to NOT contain ranges that have port numbers between 1800 and 3399 3. configdownload -vf (using the modified VF config file) This will result in an automatic cold reboot of the switch as the new repaired PORTMAP is installed.		

Defect ID:	FOS-818128		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.0a	**Technology:**	CLI
Symptom:	Switch panic when doing fosexec --fid all -cmd "portflagsshow" .		
Condition:	This occurs when running portflagsshow and it encounters an invalid data pointer on a port for unknown reasons.		
Defect ID:	FOS-818648		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1e	**Technology:**	Access Gateway
Symptom:	Windows hosts in cascaded AG G610 do not see the target disk. It can also occur in a non-cascaded AG environment but less likely		
Condition:	This is encountered in AG on G610 when bouncing ports after hareboot.		
Workaround:	Avoid bouncing ports after hareboot. Instead of port bounce, a cold boot can be done, after which port bounces are fine.		
Recovery:	Cold boot the switch.		

Defect ID:	FOS-818655		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.1a	**Technology:**	Security Policies
Symptom:	Domain ID, SCC_POLICY, port names, and port configurations reverted to the previous settings in a different environment.		
Condition:	Issue is seen after an HA update fails.		
Recovery:	Reboot the standby CP.		

Defect ID:	FOS-818669		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.1.2d	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	CLI command devicelogin --show output may reflect some ports missing from the CLI output.		
Condition:	This may occur with UCS device ports with a base address ending in 0x40 0x80 or 0xc0.		
Workaround:	Change addressing around to have these devices on ports with AL_PA=0x00.		

Defect ID:	FOS-819122		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS7.4.0a	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	Extension device may hit out of memory condition signified by the following RAS Log: XTUN-1001 FTNL Tunnel 24 Memory allocation failed tracker 3/831. The extension device may also encounter DP panics once memory is depleted.		
Condition:	Varying a FICON chipid offline when running through an extension device with FICON emulation enabled. In addition, this can be hit when hitting exception cases while running an HCL FOS upgrade. This issue is more pronounced in a large device configuration.		

Defect ID:	FOS-819311		
Technical Severity:	Low	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS7.4.2g	**Technology:**	Management GUI
Symptom:	"Professional Management tool" message reference displayed in Web Tools is no longer relevant.		

Condition:	User may see the irrelevant message when using Web Tools,.

Defect ID:	FOS-819695		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1c	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	From BNA, when the user adds the rule HA_SYNC with operator ge, g, for the active policy, the system does not generate an error as would be expected.		
Condition:	This occurs with BNA, when adding the rule HA_SYNC with operator ge, g.		

Defect ID:	FOS-819820		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1e	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	Encountered FCIP tunnels bounce between two Brocade-7810 switches during HA reboot.		
Condition:	This may occur during HA reboot in an FCIP or IP Extension routed setup if a burst of unknown packets comes in on a 7810 GE port.		

Defect ID:	FOS-819887		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1d	**Technology:**	Analytics Monitoring

Symptom:	The frequency of the stats collection has to be aligned to the wall clock's 00mts or 30mts. For example: 11:00, 11:30, 12:00, 12:30. But due to an issue in the handling of drift, the Brocade Support Link (BSL) data collection may not happen in the wall-clock aligned time, but could be random. This can impact the FA's data co-relation logic.		
Condition:	This may occur with any Time zone change or system date change (using the "date" CLI command) or any NTP server sync that results in drift greater than 30 seconds.		
Workaround:	Any Time zone change or system date change (using date command) must be accompanied by system reboot for the BSL data to be properly interpreted.		
Defect ID:	FOS-819951		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.0	**Technology:**	CLI
Symptom:	CLI command portledtest shows the test as passed but LEDs still continue to glow in any color.		
Condition:	This is seen when the action parameter is used example: portledtest -action 5, or -uports 3, or -ports 48		

Defect ID:	FOS-820023		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1a	**Technology:**	Component
Symptom:	After a hafailover, blades are no longer seen by CP with following raslog: [PLAT-1000], 5841, SLOT 6 | FFDC | CHASSIS, CRITICAL, Brocade_DCX, fabPciFindBus No PCI bus found...		
Condition:	When a FPGA blade status register bit is delayed during a hafailover window, CP interprets that as a blade is not present. This is a very rare incident.		
Recovery:	Reboot chassis recovered all blades.		

Defect ID:	FOS-820078		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1c	**Technology:**	CLI
Symptom:	fcprlsprobe timing out on shared area ports with PLOGI being sent to invalid PID ending in FF.		
Condition:	Running 'fcprlsprobe' on a port with a PID with a base AL_PA of 0x40, 0x80, or 0xc0.		
Workaround:	Run fcprlsprobe only on ports with a PID with base AL_PA of 0x00.		

Defect ID:	FOS-820169		
Technical Severity:	Low	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2b	**Technology:**	CLI
Symptom:	Man page and raslogs are updated for accuracy.		
Condition:	Missing information was added to man page, for example dnsconfig.		

Defect ID:	FOS-820206		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1c	**Technology:**	CLI
Symptom:	During script run, licenseshow command errors out.		
Condition:	When automating commands through plink (part of putty), and the return code coming from the switch for the command licenseshow is "1". This started appearing in v8.x code. Prior to that, the return code was "0".		
Workaround:	Pipe the output to "more" when running the command to get a return code of "0".		

Defect ID:	FOS-820273		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2c	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	CLI configdownload failed for filter "snmp" with "Bad Syntax" and "Failed to Parse" errors.		
Condition:	This is seen when using a configfile uploaded from FOS9.x with keys not supported in FOS8.x		

Defect ID:	FOS-820297		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1e	**Technology:**	Analytics Monitoring
Symptom:	After timezone / date change, the next day's Brocade Support Link (BSL) data collected will be interpreted incorrectly.		
Condition:	This occurs if the switch is not rebooted following timezone / date change.		

Defect ID:	FOS-820361		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.2d	**Technology:**	Component
Symptom:	Customer may encounter CP resets triggered by SysRq, along with a display of numerous "Help" messages seen on the console.		
Condition:	This results from the SysRq request that is triggered from spurious BREAK signal initiated by the Terminal Server.		

Workaround:	Run the following command on the Active and/or Standby CP. echo "0" > /proc/sys/kernel/sysrq To make this persist across CP reboots and hafailover, change the kernel.sysrq setting in /etc/sysctl.conf file from 1 to 0. (i.e This setting in /etc/sysctl.conf file should read "kernel.sysrq = 0")

Defect ID:	FOS-820436		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.2a	**Technology:**	User Accounts & Passwords
Symptom:	CLI "userconfig --change root -e yes" cannot manage the target account with error message of "conflicting LF permission".		
Condition:	This occurs when the default account parameters from user defined accounts are changed.		

Defect ID:	FOS-820627		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.1.2k	**Technology:**	Port Bring-up
Symptom:	On G610, ISL trunk cannot form or port stays in Gport after moving in/out of F-port trunk group.		
Condition:	When using 4G and 8G links on G610 platform to perform ISL or Fport-trunking.		

Defect ID:	FOS-820657		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.1.2d	**Technology:**	Web Tools
Symptom:	Switch panic or hafailover resulting from "out of memory" condition.		

Condition:	This is triggered by the termination of httpd which dumps large number of core files into memory mapped /tmp directory.

Defect ID:	FOS-820674		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2b	**Technology:**	supportShow
Symptom:	SupportSave fails from BNA.		
Condition:	Special character in the BNA password, such as "$", lead to this supportsave failure.		

Defect ID:	FOS-820710		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2	**Technology:**	Flow Vision: Flow Mirroring
Symptom:	After code upgrade, the user defined flows are not showing up in the admin level command of "flow --show";		
Condition:	This impacts all platforms running FOS8.2.2 and above.		
Workaround:	Use the "flow --show all" as admin to see the user defined flows.		

Defect ID:	FOS-820786		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2	**Technology:**	CLI
Symptom:	relayConfig CLI does not need FV(Fabric Vision) license.		
Condition:	Updated man page to removed the statement that says fabric vision license required		

Defect ID:	FOS-820837		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2b	**Technology:**	End-to-end Performance Monitoring
Symptom:	CLI "flow --show" no longer displays any of the customized flows and flow monitor deactivate fails with " ioctl failed" message.		
Condition:	This is encountered when attempting to deactivate a flow with CLI command "flow --deact" or to display a flow via "flow --show".		

Defect ID:	FOS-820856		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.1e	**Technology:**	HTTP/HTTPS
Symptom:	High CPU load observed on switch once a connection via WebTools is made with https.		
Condition:	It happens when launching WebTools on a switch using X.509 certificate.		

Defect ID:	FOS-820884		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS7.4.2g	**Technology:**	Credit Loss
Symptom:	BR6547 is not using credit value configured on peer switch using portcfgeportcredits command		
Condition:	portcfgeportcredits CLI run on a BR6547 switch may not immediately apply the specified credit. All other platforms work without issue.		
Recovery:	Cold reboot the BR6547 after running portcfgeportcredits.		

Defect ID:	FOS-820970		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Web Tools
Symptom:	Management applications (BNA, SANnav, Webtools) cannot communicate with the switch, and BSL data collection will also stop. Traffic is not impacted and operation of the switch via CLI is not impacted.		
Condition:	Issue will only be observed on GEN 5 platforms that have ASC enabled for BSL. The switch needs to also be monitored by one or more management applications. A race condition between the BSL CLI collection, data compression operation and external management applications can cause the weblinker (http demon) to hang. The likelihood of this occurring will increase with the amount of data being collected and compressed by BSL.		
Recovery:	Perform HA Reboot or HA fail-over to restart the weblinker process. This is not disruptive to traffic.		

Defect ID:	FOS-821073		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.1.2k	**Technology:**	Monitoring and Alerting Policy Suite (MAPS)
Symptom:	Customers may encounter: 1. Specific 3rd party devices flood the switch with GID_PN requests, leading to delays and impact monitoring applications. 2. Maps publishes an alert about Tx Power of SFP being 0.		
Condition:	1. The flood of GID_PN only happens on switches that have QSFP, QSFPP, QSFP28(YTA) and running FOS v8.1.2g/later, v8.2.1c/later and v8.2.2/later. 2. Maps alert can happen on any SFP type and any release.		

Defect ID:	FOS-821178		
Technical Severity:	High	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.1.2j	**Technology:**	Logging
Symptom:	Switch experience kernel panic shortly after a SupportSave command is invoked.		
Condition:	Under an unknown rare condition, the trace module is corrupted triggering switch panic.		
Workaround:	Avoid using supportsave as monitoring tool, but only use it for debug data gathering.		
Recovery:	Switch recovers itself after panic.		

Defect ID:	FOS-821268		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS9.0.0a	**Technology:**	Security Policies
Symptom:	Observed a weblinker process termination when generating certificate for HTTPS and flash space eventually went to over 90%.		
Condition:	This is encountered when Installing/deleting the https certificate while the switch is being monitored by management applications, such as SANNav.		
Workaround:	Stop the management applications, such as SANnav, that are monitoring the switch, when installing and/or deleting https certificates. It's also recommended to allow 3-4 minutes gap between generation and deletion of HTTPS certificates.		
Recovery:	Use coreshow to remove all the corefiles. If the issue is seen again, please unmonitor the switch from management application and use hareboot /hafailover to recovery.		

Defect ID:	FOS-821444		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.2d	**Technology:**	Component

Symptom:	Following an abrupt power failure on port blade, the switch continues to access the blade via PCI causing subsequent system level failures such as CP reboot, hung CP, or a blade that cannot be powered on.
Condition:	Abrupt power loss on port blade is mostly seen with SX6 port blade. Enhancements have been added in FOS v8.2.2d and later to reduce the timing window for the undesired system level side effects caused by SX6 sudden power loss.
Recovery:	Perform a hafailover and reseat of the SX6 blade.

Defect ID:	FOS-821501		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.1	**Technology:**	NPIV - N-Port ID Virtualization
Symptom:	Observed raslog NS-1012 "Detected duplicate WWPN".		
Condition:	This is encountered with an NPIV device on the first 16 ports of a FC32-48 blade in a Brocade X6-8, and when the devices on that port are bouncing frequently.		
Workaround:	Move the NPIV device to any other port 17-47.		
Recovery:	Disable the port and then enable it again.		

Defect ID:	FOS-821627		
Technical Severity:	Low	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.2d	**Technology:**	SSH - Secure Shell
Symptom:	Message of the day (MOTD) is not displayed upon connecting to the switch.		
Condition:	When MOTD is configured.		

Defect ID:	FOS-821689		
Technical Severity:	Critical	**Probability:**	Low

Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS7.4.2g	**Technology:**	Port bring up
Symptom:	Customer unable to access storage after host F-port is enabled.		
Condition:	On a 32G Logical Switch (not on Default Switch or non-VF Switch), 16G HBA with D-port feature enabled or 32G HBA with D-port and Fabric Assigned WWN feature enabled together.		
Workaround:	Disable D-port on the 16G HBA. Disable D-port or Fabric Assigned WWN feature on 32G HBA.		

Defect ID:	FOS-821746		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1c	**Technology:**	Zoning
Symptom:	Edge to edge routing was not working and frames dropped on E-port or EX-port.		
Condition:	When a port was first a F-Port and device had sent a LOGO or quickly went offline, which could leave the port in a state with a zoning flag set. When such a port is moved to a logical switch which does not have any zoning such as base switch, and the port becomes an Eport/Export, the issue will be seen on the port.		
Workaround:	Use 'filterportshow' to confirm zoning is disabled before using a port as an E-Port or EX-port.		
Recovery:	Move the port to a logical switch with zoning enabled, enable the port, and then move it back to the original logical switch.		

Defect ID:	FOS-822048		
Technical Severity:	Low	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1d	**Technology:**	CLI - Command Line Interface
Symptom:	Enhance supportsave CLI to gather ASIC register data.		

Condition:	When SupportSave is invoked.

Defect ID:	FOS-822104		
Technical Severity:	Critical	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS7.4.1	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	User may experience FCIP ingress traffic stopped due to no more internal credits available and associated C3-1014/C3-1015 RASLOG messages on a 7840 platform or C4-1014/C4-1015 RASLOG messages in a chassis with an SX6 blade. In the case of an SX6 blade, the blade will be faulted after multiple attempts to recover internal credits.		
Condition:	This stems from a timing issue either during tunnel disable or tunnel down processing where credits from FCIP back to FTNL aren't sent. This leads to permanent flow control on the peer side and the credit loss on the peer side FC ingress side.		
Workaround:	Reboot the 7840 or slot power cycle an SX6 blade.		

Defect ID:	FOS-822312		
Technical Severity:	High	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.1c	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	Performance degradation for FICON flows after FOS upgrade to FOS 8.2.1 or higher		
Condition:	When running IO over 7840 or SX6 FCIP Tunnels with FICON emulation enabled.		

Defect ID:	FOS-822411		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS

Reported In Release:	FOS8.2.1d	**Technology:**	APM - Advanced Performance Monitoring
Symptom:	BNA Dashboard and historical performance graphs may report inaccurate data.		
Condition:	There is a timing window problem in polling between software modules resulting Tx and Rx rates returned with huge junk values.		

Defect ID:	FOS-822906		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1e	**Technology:**	CLI - Command Line Interface
Symptom:	Interactive firmwaredownload presents the EULA but does not allow the user to accept it.		
Condition:	When use firmwaredownload with option "-ns", "-bs" etc.		
Workaround:	Reverse the option order via firmwaredownload "-sn", "-sb" etc., such that the "s" option is not at the end.		

Defect ID:	FOS-822935		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.2	**Technology:**	Port Bring-up
Symptom:	Occasional, a 32G LW optics port cannot come online.		
Condition:	It only happens with a specific 32G LW optics port connected to a specific server.		
Workaround:	Set the speed to 16G always work.		
Recovery:	Bounce port		

Defect ID:	FOS-822941		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS7.4.2	**Technology:**	Fastwrite
Symptom:	After a finite number of outstanding Fastwrite (FW) sequences FW processing will not generate a transfer ready sequence, but rather will shuttle the exchange (pass through mode). This will result in the pass through IOs experiencing higher IO response time when compared to the FW sequences. The FW sequence IOs will complete in as little as 1 Round Trip Time (RTT), whereas the pass through IOs will complete no sooner than 2 RTTs.		
Condition:	When using FW extended tunnels at higher IO rates and higher WAN latency, there are IOs that are passed through instead of having Transfer Ready generated.		

Defect ID:	FOS-823035		
Technical Severity:	Critical	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS
Reported In Release:	FOS8.2.2c	**Technology:**	Logging
Symptom:	Spurious power supply voltage and current readings on BR6520 or BR7840 can lead to EM-1229 and EM-1230 log messages to be displayed and the switch could be shutdown due to perceived excessive power consumption.		
Condition:	Spurious power supply readings may happen when the BR6520 or BR7840 is running with a single power supply and with FOS v8.2.2c.		
Workaround:	BR6520 or BR7840 running FOS 8.2.2c should always have two power supplies installed and operating to avoid a potential spurious power reading.		

Defect ID:	FOS-823710		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management

Reported In Release:	FOS9.0.1	**Technology:**	Routing
Symptom:	Host cannot see Lun after device login.		
Condition:	This occurs with multiple quick succession of Flogi's, as can happen with D-Port and FAPWWN, if the area binding changes during the Flogi sequence the area route is not updated correctly.		
Workaround:	Disable D-Port setting on the HBA.		
Recovery:	Upgrade to FOS with fix or disable D-Port setting on the HBA, then bounce the port, with the routing problem, to recover.		

Defect ID:	FOS-823765		
Technical Severity:	High	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1c	**Technology:**	In-flight Compression
Symptom:	Traffic disruption encountered when Encryption block errors occur due to errors, such as, "frames too long".		

Condition:	This is encountered when Frames of size 2112 or longer traverse ISLs with In-flight compression enabled. Note: 1. pre-FOS v8.0.2b, upgrades to any release are not impacted. 2. Upgrades, from FOS v8.0.2b through FOS v8.0.2f, to any FOS8.x, with the exception of FOS 8.1.0GA, exposes this problem. FOS upgrade from impacted version to a desired version may be done via FOS 8.1.0GA as an interim step to circumvent this issue. 3. Upgrades to FOS 9.x are not impacted.
Workaround:	Downgrade to v8.0.2a or prior and then upgrade to FOS v8.1.0GA before upgrading to a desired higher FOS release without this fix, or upgrade to a FOS version containing this fix.
Recovery:	Cold reboot the switch or power cycle each slot.

Defect ID:	FOS-823769		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management

Reported In Release:	FOS8.2.2c	**Technology:**	CLI
Symptom:	HA state went out of sync after duplicate "zonecreate --peerzone" and cfgadd CLIs.		
Condition:	If two zone 'add' operations are performed in parallel from two different clients, there is a chance that duplicate objects can be created in the zone database which causes the Standby CP to VERIFY during syncing operation and will cause CPs to lose sync.		
Recovery:	CLI hadisable and haenable may recover the HA state.		

Defect ID:	FOS-824494		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.2b	**Technology:**	Access Gateway
Symptom:	Switch panicked during CLI "agshow".		
Condition:	This occurs when memory that has just been freed is accessed during agshow CLI. Switch panic happens when the freed memory is reallocated by others, so it should occur infrequently.		

Defect ID:	FOS-824825		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.1	**Technology:**	SNMPv2, SNMPv3 & MIBs
Symptom:	Contact Info in SW-MIB is not correct.		
Condition:	Request to update contact information made by the PSIRT team		

Defect ID:	FOS-825365		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring/RAS

Reported In Release:	FOS7.4.2e	**Technology:**	Logging
Symptom:	Enhancement to provide periodic raslog warning messages on the impending End Of Support (EOS) for the System and remove auditdump from EOS blocked commands.		
Condition:	Currently the system terminates support functionality at EOS without any warning prior to EOS Date and auditdump is no longer available after EOS.		

Defect ID:	FOS-825388		
Technical Severity:	Critical	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2c	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	FCIP Tunnel up, but all I/O stops flowing over the tunnel and application timesout.		
Condition:	FCIP tunnel in FCR configuration has a slow leak of end to end stream credits. When the credits are exhausted, all IO is halted.		
Workaround:	Bounce the VE port(s).		

Defect ID:	FOS-825673		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	Virtualization
Reported In Release:	FOS8.1.2k	**Technology:**	Access Gateway
Symptom:	Port is disabled with the reason of: Disabled (LD SFP is not supported in AG mode)		
Condition:	Issue will be seen when the port with LW SFP is coming online in AG on FOS v8.x and FOS v9.x		

Defect ID:	FOS-825690		
Technical Severity:	Medium	**Probability:**	High

Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.1.2	**Technology:**	Platform Services
Symptom:	The chassis management module does not show the FOS version.		
Condition:	This only impacts Brocade6546 platform.		
Defect ID:	FOS-825979		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS9.0.1	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP service crashes and restarts.		
Condition:	Issue is seen if invalid input is provided for "context" when making SNMPv3 query		
Workaround:	Provide a valid "context" in format following format - "VF:<vf id>"		

Defect ID:	FOS-826094		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS9.0.1	**Technology:**	FCIP
Symptom:	connUnitPortStatus trap not getting generated during VE portdisable.		
Condition:	issue is seen when ve port is disabled		

Defect ID:	FOS-826163		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS9.0.0b	**Technology:**	Component
Symptom:	Fanshow/sensorshow shows "Below minimum" instead of "Faulty".		

Condition:	This is seen upon removal and reinsertion of PS with integrated FAN. And also during disruptive testing of the FAN by deliberate insertion of an object to stop the FAN.

Defect ID:	FOS-826172		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	Security
Reported In Release:	FOS8.2.2	**Technology:**	LDAP - Lightweight Directory Access Protocol
Symptom:	If a user role is created with upper and lower case characters, it is stored as lowercase. However, when specifying a role under the ldapcfg command it does not do the same conversion.		
Condition:	When using ldapcfg command, the role is not converted to lowercase when it is used along with map attributes.		

Defect ID:	FOS-826256		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Extension
Reported In Release:	FOS8.2.2c	**Technology:**	FCIP - Fibre Channel over IP
Symptom:	FX8-24 logging repeated circuit offline/online events until a hang.		
Condition:	After FX8-24 blade takes a panic with an invalid memory accessing		
Recovery:	Reboot of the FX8-24 blade on one or both sides		

Defect ID:	FOS-826747		
Technical Severity:	Medium	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1c	**Technology:**	Component

Symptom:	A port blade failed and went missing from the "slotshow" CLI and switch monitor components such as maps continue to report system status as healthy.
Condition:	This happens when a blade cannot be seen on a PCI bus. Blade should be faulted in this rare scenario such that switch monitor software can report proper status.
Recovery:	Reseat or replace port blade.

Defect ID:	FOS-826804		
Technical Severity:	High	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Monitoring
Reported In Release:	FOS8.2.1d	**Technology:**	MAPS - Monitoring and Alerting Policy Suite
Symptom:	Switch needs a manual reboot to recover from HA Out of Sync state after mdd daemon panic. Observed raslog: [HAM-1013], , SLOT 1 | CHASSIS, CRITICAL, , Can't restart (md (pid=27115)): System unready or LS trans in progress. Reboot/Failover manually if necessary.		
Condition:	During a re-balance action to bring the port group into a balanced state when connecting to a 3rd party switch.		

Defect ID:	FOS-827342		
Technical Severity:	Medium	**Probability:**	High
Product:	Fabric OS	**Technology Group:**	System
Reported In Release:	FOS8.2.1c	**Technology:**	CLI
Symptom:	Switch reports class-3-discards value as 4294967295 after clearing port stats.		
Condition:	After CLI portstatsclear is ran.		

16.7 Closed without Code Changes in 8.2.3

Defect ID:	FOS-810839	**Technical Severity:**	High
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Management
Reported In Release:	FOS8.2.1	**Technology:**	Fibre Channel Services
Symptom:	Switch rebooted after it ran out of memory.		
Condition:	Misbehaving device sending invalid values for FC header sequence count and sequence ID leads to out-of-memory condition.		
Workaround:	Identify the misbehaving devices and remove them from the fabric.		
Recovery:	The reboot that results from out-of-memory recovers the switch. If high IU memory usage is detected before the out-of-memory condition, hafailover can temporarily recover and prevent the unexpected switch reboot.		

Defect ID:	FOS-816098	**Technical Severity:**	Low
Reason Code:	Already Fixed in Release	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.2.1	**Technology:**	Other
Symptom:	Raslog TS-1001, indicating NTP Query Failed, occurs daily or weekly.		
Condition:	The switch's clock server is configured to an external NTP server.		
Workaround:	Configure switch's clock server to a stable NTP clock server or else confirm the network stability if issue persists.		

Defect ID:	FOS-820194	**Technical Severity:**	High
Reason Code:	Implemented	**Probability:**	Low
Product:	Fabric OS	**Technology Group:**	Traffic Management
Reported In Release:	FOS8.2.1c	**Technology:**	FSPF - Fabric Shortest Path First

Symptom:	FSPF daemon crashes and causes failover.
Condition:	This occurs when EX-port trunk is coming online.
Workaround:	Enable the EX-port trunk only when the switch is not busy, to avoid this rare timing issue.
Recovery:	The failover does automatically recover the trunk.

Defect ID:	FOS-826750	**Technical Severity:**	Medium
Reason Code:	Already Fixed in Release	**Probability:**	null
Product:	Fabric OS	**Technology Group:**	Other
Reported In Release:	FOS8.2.2c	**Technology:**	Other
Symptom:	SNMP incorrectly reporting uptime of 497 days due to deprecation of switchuptime CLI command.		
Condition:	This is a rare occurrence and may be encountered while performing a firmwarecleaninstall, or when a new switch is first installed with FOS8.2.2x.		

Revision History

Version	Summary of changes	Publication date
1.0	Initial document version.	4/14/2023
2.0	Added defects (listed) to the CWC table which erroneously were not included when generating the table for version 1 of the Release Notes: 842145, 841520, 843045, 844942 and 843589.	5/23/2023
3.0	Updated Security Vulnerability Fixes with CVEs available for public disclosure.	8/1/2023


BROCADE
A Broadcom Company