CERT Advisories - A Compilation of AIX Advisories

CERT Advisory (10/17/91) on TFTP Vulnerability 2

CERT Advisory (03/05/92) on REXD Vulnerability 5

CERT Advisory (03/31/92) on /bin/passwd Vulnerability 7

CERT Advisory (04/27/94) on Anonymous FTP 9

CERT Advisory (05/26/92) on crontab Vulnerability 11

CERT Advisory (03/17/94) on Performance Tools 13

CERT Advisory (05/23/94) on login Vulnerability 15

CERT Advisory (06/03/94) on bsh Vulnerability 19

CERT Advisory (10/17/91) on TFTP Vulnerability

About this Document

This document is based on the CERT advisory issued October 17, 1991, about an AIX TFTP daemon vulnerability.

Overview

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the TFTP daemon in all versions of AIX for IBM RISC System/6000 machines.

IBM is aware of this problem and a fix is available as APAR number IX22628. This patch is available for all AIX releases from "GOLD" to the current release.

Note: This is an updated patch from one recently made available and fixes a security hole in the original patch. The SCCS ID of the correct patch is tftpd.c 1.13.1.3 (*not* 1.13.1.2 or earlier versions). This can be checked using the following "what" command.

```
% what /etc/tftpd
/etc/tftpd:
   56      1.13.1.3  tftpd.c, tcpip, tcpip312 10/10/91 09:01:48
   tftpsubs.c   1.2  com/sockcmd/tftpd,3.1.2,9048312 10/8/89 17:40:55
```

Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

The fix will appear in the upcoming 2009 update and the next release of AIX.

I. Description

Previous versions of tftpd did not provide a method for restricting TFTP access.

II. Impact

If TFTP is enabled at your site, anyone on the Internet can retrieve copies of your site's world-readable files, such as /etc/passwd.

III. Solution

For Sites That Do Not Need to Allow TFTP Access

Sites that do not need to allow tftp access should disable it. This can be done by editing /etc/inetd.conf and deleting or commenting out the tftpd line:

```
#tftp     dgram     udp    wait    nobody  /etc/tftpd     tftpd -n
```

and then, as root, restarting inetd with the "refresh" command.

```
# refresh -s inetd
```

For more details on starting/stopping tftp, refer to documentation for the System Resource Controller (SRC) or the System Management Interface Tool (SMIT).

For Sites That Must Run TFTPD

Sites that must run tftpd (for example, to support X terminals) should obtain and install the above patch AND create a /etc/tftpaccess.ctl file to restrict the files that are accessible. The /etc/tftpaccess.ctl file should be writable only by root. Although the new /etc/tftpaccess.ctl mechanism provides a very general capability, the CERT/CC strongly recommends that sites keep this control file simple. For example, the following tftpaccess.ctl file is all that is necessary to support IBM X terminals:

```
# /etc/tftpaccess.ctl
# By default, all files are restricted if /etc/tftpaccess.ctl exists.
# Allow access to X terminal files.
allow:/usr/lpp/x_st_mgr/bin
```

Note: Be CERTAIN to create the /etc/tftpaccess.ctl file. If it does not exist then all world-readable files are accessible as in the current version of tftpd.

Installation Instructions:

1. Create an appropriate /etc/tftpaccess.ctl file.
2. From the directory containing the new tftpd module, issue the following commands as root.

```
# chmod 644 /etc/tftpaccess.ctl
# chown root.system /etc/tftpaccess.ctl
# mv /etc/tftpd /etc/tftpd.old
# cp tftpd /etc
# chmod 755 /etc/tftpd
# chown root.system /etc/tftpd
# refresh -s inetd
```

Thanks

The CERT/CC wishes to thank Karl Swartz of the Stanford Linear Accelerator Center for bringing this vulnerability to our attention.

If You Believe Your System Has Been Compromised

If you believe that your system has been compromised, contact CERT/CC via telephone or e-mail.

```
Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 24-hour hotline:
        CERT/CC personnel answer 7:30a.m.-6:00p.m. EST/EDT,
        on call for emergencies during other hours.
```

Other Information

Past advisories and other computer security related information are available for anonymous ftp from the cert.org (192.88.209.5) system.

CERT Advisory (03/05/92) on REXD Vulnerability

About this Document

This document is based on the CERT advisory issued March 5, 1992, about an AIX REXD daemon vulnerability.

Overview

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability with the rexd daemon in versions 3.1 and 3.2 of AIX for IBM RISC System/6000 machines.

IBM is aware of the problem and it will be fixed in future updates to AIX 3.1 and 3.2. The fix number is IX21353.

Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

Patches may be obtained outside the U.S. by contacting your local IBM representative.

The fix is also provided below.

I. Description

In certain configurations, particularly if NFS is installed, the rexd (RPC remote program execution) daemon is enabled.

Note: Installing NFS with the current versions of "mknfs" will re-enable rexd even if it was previously disabled.

II. Impact

If a system allows rexd connections, anyone on the Internet can gain access to the system as a user other than root.

III. Solution

CERT/CC and IBM recommend that sites take the following actions immediately. These steps should also be taken whenever "mknfs" is run.

1. Be sure the rexd line in /etc/inetd.conf is commented out with a "#" at the beginning of the line:

```
#rexd  sunrpc_tcp tcp  wait  root  /usr/etc/rpc.rexd rexd 100017 1
```

2. Refresh inetd by running the following command as root:

```
refresh -s inetd
```

Thanks

The CERT/CC wishes to thank Darren Reed of the Australian National University for bringing this vulnerability to our attention and IBM for their response to the problem.

If You Believe Your System Has Been Compromised

If you believe that your system has been compromised, contact CERT/CC or your representative in FIRST (Forum of Incident Response and Security Teams).

```
Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
  CERT/CC personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4),
  on call for emergencies during other hours.

Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
```

Other Information

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous ftp from cert.org (192.88.209.5).

CERT Advisory (03/31/92) on /bin/passwd Vulnerability

About this Document

This document is based on the CERT advisory issued March 31, 1992, on an AIX /bin/passwd vulnerability.

Overview

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability with the passwd command in AIX 3.2 and the 2007 update of AIX 3.1.

IBM is aware of this problem, and a fix is available as APAR number IX23505. Patches are available for AIX 3.2 and the 2007 update of AIX 3.1.

The fix can be received in either of these ways:

- Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

  You may obtain patches outside the U.S. by contacting your local IBM representative.

- If you are on the Internet, use anonymous ftp to obtain the fix from software.watson.ibm.com.

  ```
  Patch          Filename                Checksum
  AIX 3.2        pub/aix3/pas.32.tar.Z   54431  2262
  AIX 3.1 2007   pub/aix3/pas.31.tar.Z   06703    99
  ```

  Patches should be retrieved using binary mode.

IBM is currently incorporating the fix into the 3.2 version and 3.1 updates of AIX. Future shipments of these products should not be vulnerable to this problem. If you have any questions about products you receive, please contact your IBM representative.

I. Description

The passwd command contains a security vulnerability.

II. Impact

Local users can gain unauthorized root access.

III. Solution

1. As root, disable /bin/passwd until you obtain and install the patch.

```
# chmod 0500 /bin/passwd
```

2. Obtain the fix from IBM and install according to the directions provided with the patch.

Thanks

The CERT/CC would like to thank Paul Selick of the University of Toronto for bringing this security vulnerability to our attention. We would also like to thank IBM for their quick response to this problem, and for making the patches available via anonymous ftp.

If You Believe Your System Has Been Compromised

If you believe that your system has been compromised, contact CERT/CC or your representative in FIRST (Forum of Incident Response and Security Teams).

```
Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
  CERT/CC personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4),
  on call for emergencies during other hours.

Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
```

Other Information

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous ftp from cert.org (192.88.209.5).

CERT Advisory (04/27/94) on Anonymous FTP

About this Document

This document is based on the CERT advisory issued April 27, 1992, about an AIX anonymous FTP vulnerability.

Overview

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the anonymous FTP configuration in all versions of AIX.

IBM is aware of this problem and a fix is available as APAR number IX23944. This patch is available for all AIX releases from "GOLD".

Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

You can obtain patches outside the U.S. by contacting your local IBM representative. The fix will appear in the upcoming 2009 update and the next release of AIX.

I. Description

Previous versions of the anonymous FTP installation script, /usr/lpp/tcpip/samples/anon.ftp, incorrectly configured various files and directories.

II. Impact

Remote users can execute unauthorized commands and gain access to the system if anonymous FTP has been installed.

III. Solution

1. Obtain the fix from IBM Support. The fix contains three files: a "readme" file (README.a23944), the fix installation script (install.a23944), and an archive containing the updated files (PATCH.a23944.Z).
2. Install the fix following the instructions in the README file.

Thanks

The CERT/CC would like to thank Charles McGuire of the Computer Science Department, the University of Montana, for bringing this security vulnerability to our attention and IBM for their response to the problem.

If You Believe Your System Has Been Compromised

If you believe that your system has been compromised, contact CERT/CC or your representative in FIRST (Forum of Incident Response and Security Teams).

```
Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
  CERT/CC personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4),
  on call for emergencies during other hours.

Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
```

Other Information

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous ftp from cert.org (192.88.209.5).

CERT Advisory (05/26/92) on crontab Vulnerability

About This Document

This document is based on the CERT advisory issued May 26, 1992, about a AIX crontab vulnerability.

Overview

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in crontab(1) in version 3.2 of IBM's AIX operating system.

IBM is aware of this problem and a fix is available as APAR number IX26997 for AIX version 3.2. The version information for the patched /usr/bin/crontab is shown in the following what(1) output:

```
% what /usr/bin/crontab
04 1.23 com/cmd/cntl/cron/crontab.c, cmdcntl, bos320, 9218320f 4/8/92 11:50:42
07 1.8  com/cmd/cntl/cron/permit.c, bos, bos320 4/25/91 17:16:59
11 1.15  com/cmd/cntl/cron/cronsub.c, bos, bos320 8/18/91 20:42:32
06 1.9  com/cmd/cntl/cron/funcs.c, bos, bos320 6/8/91 21:22:40
```

If your crontab contains older modules than the above output indicates, we suggest that you install the fix.

I. Description

The distributed version of /usr/bin/crontab contains a security vulnerability.

II. Impact

Local users can gain unauthorized root access to the system.

III. Solution

The CERT/CC suggests that sites install the fix that IBM has made available. As an interim step, we suggest that sites prevent all non-root users from running /usr/bin/crontab by removing (or renaming) the /var/adm/cron/cron.allow and /var/adm/cron/cron.deny files.

1. Obtain the fix from IBM Support:

- Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

  Patches may be obtained outside the U.S. by contacting your local IBM representative.

- If you are on the Internet, use anonymous ftp to obtain the fix from software.watson.ibm.com (129.34.139.5).

  ```
  Patch           Filename                Checksum
  AIX 3.2         pub/aix3/cronta.tar.Z   02324   154
  ```

  The patch must be retrieved using binary mode.

2. Install the fix following the instructions in the README file.

Thanks

The CERT/CC would like to thank Fuat Baran of Advanced Network & Services, Inc. for bringing this security vulnerability to our attention and IBM for their quick response to this problem.

If You Believe That Your System Has Been Compromised

If you believe that your system has been compromised, contact CERT/CC or your representative in FIRST (Forum of Incident Response and Security Teams).

```
Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
  CERT/CC personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4),
  on call for emergencies during other hours.

Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
```

Other Information

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous ftp from cert.org (192.88.209.5).

CERT Advisory (03/17/94) on Performance Tools

About this Document

This document is based on the CERT advisory issued February 24, 1994, on AIX performance tools vulnerabilities.

Overview

The CERT Coordination Center has received information concerning vulnerabilities in the "bosext1.extcmds.obj" Licensed Program Product (performance tools). These problems exist on IBM AIX 3.2.4 systems that have Program Temporary Fixes (PTFs) U420020 or U422510 installed and on all AIX 3.2.5 systems.

CERT recommends that affected sites apply the workaround provided in section III below.

I. Description

Vulnerabilities exist in the bosext1.extcmds.obj performance tools in AIX 3.2.5 and in those AIX 3.2.4 systems with Program Temporary Fixes (PTFs) U420020 or U422510 installed. These problems do not exist in earlier versions of AIX.

II. Impact

Local users can gain unauthorized root access to the system.

III. Workaround

- The recommended workaround is to change the permissions of all the programs in the /usr/lpp/bosperf directory structure so that the setuid bit is removed and the programs can be executed only by "root". This can be accomplished as follows:

  ```
  % su root
  # chmod -R u-s,og= /usr/lpp/bosperf/*
  ```

  The programs affected by this workaround include:

  ```
  filemon, fileplace, genkex, genkld, genld, lvedit,
  netpmon, rmap, rmss, stripnm, svmon, tprof
  ```

  As a result of this workaround, these programs will no longer be executable by users other than "root".

- Patches for these problems can be ordered as Authorized Program Analysis Report (APAR) IX42332.

  Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

  You may obtion APARs outside the U.S. by contacting your local IBM representative.

  Any further information that we receive on APAR IX42332 will be available by anonymous FTP in the file pub/cert_advisories/CA-94:03.README on info.cert.org.

Thanks

The CERT Coordination Center wishes to thank Jill K. Bowyer of USAF/DISA for reporting this problem and IBM for their prompt response to this problem.

If You Believe Your System Has Been Compromised

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in Forum of Incident Response and Security Teams (FIRST).

```
Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
  CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
  and are on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
```

Other Information

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous FTP on info.cert.org.

CERT Advisory (05/23/94) on login Vulnerability

About this Document

This document is based on the CERT advisory issued May 23, 1994, about a vulnerability in /bin/login. (The appendix included here is the version issued with the advisory. You can obtain the latest update via anonymous FTP from info.cert.org.)

Overview

The CERT Coordination Center has learned of a vulnerability in /bin/login. This vulnerability potentially affects all IBM AIX 3 systems and Linux systems. At this time, we believe that only IBM AIX 3 and Linux systems are at risk.

Included with this advisory is an appendix containing the CA-94:09.README, which lists the vendors who have responded to our inquiries and the status of their investigation into this vulnerability report. As we receive additional information relating to this advisory, we will place it, along with any clarifications, in the README file, available via anonymous FTP from info.cert.org. We encourage you to check the README files regularly for updates on advisories that relate to your site.

IBM AIX Vulnerability

Description

A vulnerability exists in /bin/login on all IBM AIX 3 systems.

Impact

Remote users can obtain unauthorized root access on the affected hosts.

Solution

IBM is working on an official fix, which is still under development. The reference number for this fix is APAR IX44254. Until you obtain the official fix from IBM, we encourage you to apply the workaround or install the emergency fix below.

Workaround

The recommended workaround is to disable the rlogin daemon:

1. As root, edit "/etc/inetd.conf". Comment out the line "login ... rlogin".
2. Run "inetimp".
3. Run "refresh -s inetd".

Emergency Fix

The emergency fix for the different levels of AIX 3 affected by this vulnerability is available via anonymous FTP from software.watson.ibm.com:/pub/rlogin/rlogin.tar.Z. Installation instructions are included in the README file (which is included in rlogin.tar.Z).

Checksum information for rlogin.tar.Z:

```
BSD:      25285   317
SystemV:  13021 633 rlogin.tar.Z
MD5:      MD5 (rlogin.tar.Z) = 803ee38c2e3b8c8c575e2ff5e921034c
```

Official Fix

The official fix for this problem can be ordered as APAR IX44254.

Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

You may obtain APARs outside the U.S. by contacting your local IBM representative.

Linux vulnerability

Description

A vulnerability exists in /bin/login for Linux systems.

Impact

Any user, remote or local, can obtain unauthorized root access on the affected hosts.

Solution

A patch that addresses the remote access problem has been made available via anonymous FTP from sunsite.unc.edu:

```
/pub/Linux/system/Network/sunacm/URGENT/README.security
/pub/Linux/system/Network/sunacm/URGENT/security.tgz
```

The "security.tgz" file includes other security fixes in addition to the /bin/login patch.

Checksum information for README.security:

```
BSD:      09575     1
SystemV:  20945 1 README.security
MD5:      MD5 (README.security) = 41d14d7b8725c7a1015adeb49601619b
```

Checksum information for security.tgz:

```
BSD:      32878   257
SystemV:  40797 513 security.tgz
MD5:      MD5 (security.tgz) = dd4585cf4da1b52d25d619bf45f55b75
```

To address the local access problem, we encourage you to install a version of /bin/login that does not allow the -f option in the form "-f<user>", but only allows this option in the form "-f <user>", as two arguments. At this time, we do not know which versions of login.c are vulnerable. As we receive additional information, we will update the CA-94:09.README file. Again, we encourage you to check this README file regularly for updates.

Thanks

The CERT Coordination Center wishes to thank Axel Clauberg of University of Cologne for reporting the IBM AIX problem, and IBM for their assistance in responding to this problem.

If You Believe Your System Has Been Compromised

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT via electronic mail, CERT strongly advises that the e-mail be encrypted. CERT can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT for details).

```
Internet E-mail: cert@cert.org

Telephone:       412-268-7090 (24-hour hotline)
    CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
    and are on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
USA
```

Past advisories and their associated README files, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from info.cert.org.

Appendix — CA-94:09.README

This file is a supplement to the CERT Advisory CA-94:09.bin.login.vulnerability of May 23, 1994, and will be updated as additional information becomes available.

We have received feedback from these vendors, who indicated that their products are not vulnerable:

```
Amdahl
Apple
BSD
BSDI
Harris
HP
Motorola
NeXT
Pyramid
SCO
SGI
Solbourne
Sony
Sun
```

CERT has verified that the following vendor products are not vulnerable:

```
Free BSD
```

We have received feedback from these vendors, who have made patches available to address the /bin/login vulnerability:

```
IBM
  workaround:       see "Workaround" on page 15
  emergency patch:  software.watson.ibm.com:/pub/rlogin/rlogin.tar.Z
  Official patch:   APAR IX44254

Linux
  patch:  sunsite.unc.edu:/pub/Linux/system/Network/sunacm/URGENT/*
```

CERT Advisory (06/03/94) on bsh Vulnerability

About this Document

This document is based on the CERT advisory issued June 3, 1994, about a AIX bsh vulnerability.

Overview

The CERT Coordination Center has learned of a vulnerability in the batch queue (bsh) of IBM AIX systems running versions prior to and including AIX 3.2.

CERT recommends disabling the batch queue by following the workaround instructions in Section III below. Section III also includes information on how to obtain fixes from IBM if the bsh queue functionality is required by remote systems.

As we receive additional information relating to this advisory, we will place it, along with any clarifications, in a CA-94:10.README file. CERT advisories and their associated README files are available by anonymous FTP from info.cert.org. We encourage you to check the README files regularly for updates on advisories that relate to your site.

I. Description

The queueing system on IBM AIX includes a batch queue, "bsh", which is turned on by default in /etc/qconfig on all versions of AIX 3 and earlier.

II. Impact

If network printing is enabled, remote and local users can gain access to a privileged account.

III. Solution

In the next release of AIX, the bsh queue will be turned off by default. CERT recommends that the bsh queue be turned off using the workaround described in Section A below unless there is an explicit need to support this functionality for remote hosts. If this functionality must be supported, IBM provides fixes as outlined in Sections B and C below. For questions concerning these workarounds or fixes, please contact IBM at the number provided below.

A. Workaround

Disable the bsh queue by following one of the two procedures outlined below:

- As root, from the command line, enter:

```
# chque -qbsh -a"up = FALSE"
```

- From SMIT, enter:

```
- Spooler
- Manage Local Printer Subsystem
- Change/Show Characteristics of a Queue
    select bsh
- Activate the Queue
    select no
```

B. Emergency fix

Obtain and install the emergency fix for the version(s) of AIX used at your site. Fixes for the various levels of AIX are available by anonymous FTP from software.watson.ibm.com. The files are located in /pub/aix/bshfix.tar.Z in compressed tar format. Installation instructions are included in the README file included as part of the tar file.

The directory /pub/aix contains the latest available emergency fix for APAR IX44381. As updates become available, any new versions will be placed in this directory with the name bshfix<#>.tar.Z with <#> being incremented for each update. See the README.FIRST file in that directory for details.

IBM may remove this emergency fix file without prior notice if flaws are reported. Due to the changing nature of these files, no checksum information is available.

C. Official fix

The official fix for this problem can be ordered as APAR IX44381.

Fixes (PTFs) for AIX 3.2.5 and later can be downloaded via Internet with the FixDist service. For FixDist information and instructions, order fax number 1228 from 1-800-IBM-4FAX. If you don't have access to Internet or if your machine is at a pre-3.2.5 AIX level, you can request a specific fix number from 1-800-CALL-AIX. All other services from 1-800-CALL-AIX which are not Program Services require a software support contract.

To obtain APARs outside of the U.S., contact your local IBM representative.

Thanks

The CERT Coordination Center wishes to thank Gordon C. Galligher of Information Resources, Inc. for reporting this problem and IBM Corporation for their support in responding to this problem.

If You Believe Your System Has Been Compromised

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT via electronic mail, CERT strongly advises that the e-mail be encrypted. CERT can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT for details).

```
Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
  CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
  and are on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
USA
```

Other Information

Past advisories and their associated README files, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from info.cert.org.

Reader's Comments

Please fax this form to (512) 823-5972, attention "AIXServ Information".

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX (415-855-4329 outside U.S., from fax machine phone).

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

END OF DOCUMENT (cert.all.gen, 4FAX# 1450)