MOTOROLA SOLUTIONS

DOCUMENT NUMBER: MTN-0009-20-NA
APC: 202
ISSUE DATE: 02-2020
EXPIRATION DATE: 29-02-2021
Bulletin Type: Informational Only

Motorola Solutions Technical Notification (MTN)

TITLE: VxWorks Operating System Upgrade and Patch for MCD 5000 Deskset System

TECHNOLOGY: Astro Conventional and Trunked - VoIP Technology

SYMPTOMS:
VxWorks Operating System Vulnerability issue identified with Release 6.8 in July 2019. This could allow an attacker to take over devices with no user interaction required and bypass perimeter security devices such as firewalls and network address translation (NAT)
Solutions.

	Critical	
1	CVE-2019-12256 (V7NET-2423) : Stack overflow in the parsing of IPv4 packets' IP options	VxWorks 6.8 Not Vulnerable
2	CVE-2019-12255 (VXW6-87100) : TCP Urgent Pointer = 0 leads to integer underflow	VxWorks 6.8 Vulnerable
3	CVE-2019-12260 (V7NET-2425) : TCP Urgent Pointer state confusion caused by malformed TCP AO option	VxWorks 6.8 Not Vulnerable
4	CVE-2019-12261 (V7NET-2425) : TCP Urgent Pointer state confusion during connect() to a remote host	VxWorks 6.8 Vulnerable
5	CVE-2019-12263 (V7NET-2425) : TCP Urgent Pointer state confusion due to race condition	VxWorks 6.8 Vulnerable
6	CVE-2019-12257 (VXW6-87101) : Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc	VxWorks 6.8 Vulnerable
	Other	
1	CVE-2019-12258 (V7NET-2426) : DoS of TCP connection via malformed TCP options	VxWorks 6.8 Vulnerable
2	CVE-2019-12262 (V7NET-2427) : Handling of unsolicited Reverse ARP replies (Logical Flaw)	VxWorks 6.8 Vulnerable
3	CVE-2019-12264 (V7NET-2428) : Logical flaw in IPv4 assignment by the ipdhcpc DHCP client	VxWorks 6.8 Vulnerable
4	CVE-2019-12259 (V7NET-2428) : DoS via NULL dereference in IGMP parsing	VxWorks 6.8 Vulnerable
5	CVE-2019-12265 (V7NET-2428) : IGMP Information leak via IGMPv3 specific membership report	VxWorks 6.8 Vulnerable

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:
Deskset model F2380A; RGU models F7979A and F7879B. All releases impacted: 1.0, 2.0, 2.1, 2.2, 2.2.1, 2.3, 2.3.2, 2.3.3

SEVERITY RECOMMENDATION:
High / Safety - Perform Immediately - This applies to customer's with large systems who operate in open systems.
Medium / Operational - This applies to small customers who operate in closed systems where vulnerability is very low risk. Schedule to implement

ROOT CAUSE / DEFINITIVE TEST:
Armis released their public disclosure of 11 vulnerabilities for WindRivers VxWorks real time operating system (RTOS), which could allow an attacker to take over devices with no user interaction required, and bypass perimeter security devices such as firewalls and network address translation (NAT) solutions. The MCD 5000 deskset is impacted by 9 of the 11 vulnerabilities identified.

WORKAROUNDS AND CORRECTIVE ACTIONS:
Upgrade to version 2.3.5 or later release.

RESOLUTIONS AND REPAIR PROCEDURES:
Upgrade the MCD5000 to 2.3.5 or later release by following the procedures in the Installation Guide. A valid license is required for access to updated software.

PARTS REQUIRED (HARDWARE/SOFTWARE):
MCD5000 Deskset 2.3.5 firmware can be downloaded from MOL:
http://motonline.mot-solutions.com/

Resource Center→Software→Two-Way→Dispatch Console→MCD 5000 Deskset System
File Name : MCD 5000 R2.3.5 FIRMWARE UPDATE

ADDITIONAL INFORMATION:

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:

WHEN TO APPLY RESOLUTION:
After reboot __
After (re)installation __
After upgrade __
After power cycle __
After database restoration __
After failure __
On FRU replacement __
During maintenance __
Immediately __
As instructed _x_
Information only __

LABOR ALLOWANCE:
This is an informational bulletin. No labor warranty is implied, intended or authorized for U.S. Domestic Partners/Customers. Other regions should follow their own standard procedures.

For assistance with this bulletin please contact your MSI Technical support center
https://www.motorolasolutions.com/en_us/support.html