SECURITY ADVISORY – Urgent/11 Vulnerabilities in VxWorks® Operating System and Polycom Products

Advisory Version 1.0

DATE PUBLISHED: December 19th, 2019

ANY INFORMATION IN THIS ADVISORY IS SUBJECT TO CHANGE.

Please Note: Poly takes the security of our customers and our products seriously. This is a living document and may be subject to updates. The latest version of this document can be found at the following URL:

https://support.polycom.com/content/support/security-center.html

Vulnerability Summary

Researchers at security vendor Armis Labs discovered 11 vulnerabilities in the Wind River Systems' VxWorks® Operating System, which is used in certain Poly voice endpoints. Dubbed "URGENT/11," the vulnerabilities reside in VxWorks' IPnet TCP/IP stack and impact all versions of the VxWorks® Operating System since version 6.5.

URGENt/11 is made up of the following CVEs:

CVE Number	Severity	Type	Notes
CVE-2019-12256	9.8	TCP/IP Stack	Stack overflow in the parsing of IPv4 packets' IP options
CVE-2019-12257	8.8	DHCP Client	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc
CVE-2019-12255	9.8	TCP Urgent Pointer	TCP Urgent Pointer = 0 leads to integer underflow
CVE-2019-12260	9.8	TCP Urgent Pointer	TCP Urgent Pointer state confusion caused by malformed TCP AO option

CVE-2019-12261	8.8	TCP Urgent Pointer	TCP Urgent Pointer state confusion during connect() to a remote host
CVE-2019-12263	8.1	TCP Urgent Pointer	TCP Urgent Pointer state confusion due to race condition
CVE-2019-12258	7.5	TCP Connection	DoS of TCP connection via malformed TCP options
CVE-2019-12259	6.3	TCP/IP Stack	DoS via NULL dereference in IGMP parsing
CVE-2019-12262	7.1	ARP Handler	Handling of unsolicited Reverse ARP replies (Logical Flaw)
CVE-2019-12264	7.1	DHCP	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client
CVE-2019-12265	5.4	IGMP	IGMP Information leak via IGMPv3 specific membership report

Products Affected

This set of vulnerabilities affects Polycom SoundPoint and SoundStation products running the UCS 4.1 software family. It does **not** affect endpoints running the UCS 4.0 software family.

Solution

Poly's UCS software version 4.1.1.0934 rts11 AB addresses these vulnerabilities. Endpoints running the UCS 4.1 software should update their devices with this software, which can be downloaded from the Poly Support website at:

https://support.polycom.com/content/support/north-america/usa/en/support/voice.html

CVSS v3 Base Metrics

To assist our customers in the evaluation of this vulnerability, Poly uses the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

Base CVSS v3 Scores

CVE-2019-12256	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-12257	8.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-12255	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-12260	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-12261	8.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-12263	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-12258	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2019-12259	6.3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2019-12262	7.1	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2019-12264	7.1	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
CVE-2019-12265	5.4	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

For more information on CVSS v3 please see: *https://www.first.org/cvss*

Severity: High

Rating	Definition
Critical	A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.
High	A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.
Medium	A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.
Low	A vulnerability that has minimal impact to the system and is extremely difficult to exploit.

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit:

https://support.polycom.com/content/support/security-center.html For the latest information.

You might also find value in the high-level security guidance and security news located at:

https://support.polycom.com/content/support/security-center.html

Revision History

Revision 1.0 - Original publication: December 19th, 2019