SECURITY ADVISORY – Processor based “Speculative Execution” Vulnerabilities AKA “Spectre” and “Meltdown” – Version 1.3

Security Advisory Relating to the “Speculative Execution” Vulnerabilities with some microprocessors

DATE PUBLISHED: January 10th, 2018

This information applies to Polycom products and the “Spectre” and “Meltdown” vulnerabilities. Polycom is continuing to investigate the impact to our product line to determine which products may be affected by these vulnerabilities and will release patches or confirmation of non-vulnerability on a product-by-product basis.

Any information in this Advisory is subject to change as our investigation progresses.

Please Note: This is a living document, and Polycom will update this advisory regularly as the investigation progresses and new information becomes available. The newest version of this document will always reside at the following URL:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

Vulnerability Summary

Speculative Execution Vulnerabilities, aka “Spectre” and “Meltdown” – CVE-2017-5753, CVE-2017-5715, CVE-2017-5754

On January 3, 2018 researchers disclosed information on three vulnerabilities identified in some microprocessors that could allow an attacker to exploit processor speculation or take advantage of cache timing side-channels. Under specific circumstances, these vulnerabilities could potentially allow unprivileged local attacker to read privileged data contained in secure areas of system memory belonging to other processes or system kernel.

Impact and Risk

Polycom is investigating and will continue to investigate all products and product lines to determine if any allow exploitation of unprivileged reading of secure data in memory. Polycom uses a wide variety of microprocessors across our products and does not typically disclose the specific CPUs used in a specific product.

Mitigations

The impact of these vulnerabilities is greatest on multi-user systems – shared hosting, cloud services, virtual machines, etc. – where unprivileged access to the system resources is generally available. For an attacker to exploit these vulnerabilities, an attacker must be able to execute malicious code on a vulnerable device. Polycom products are designed to mitigate such classes of vulnerability, are not multi-user systems, and do not typically allow access to the operating system for normal operation nor do they allow the installation of custom code, largely mitigating the vulnerabilities.

Some Polycom infrastructure products do by default provide unprivileged OS-level service accounts for configuration and maintenance. On these systems, we recommend changing default passwords and restricting account access to trusted administrators.

Products

Group Series	Vulnerable
Centro	Vulnerable
Medialign	Vulnerable
Debut	Investigating
HDX	Not Vulnerable
Pano	Vulnerable
RealPresence Desktop and Mobile (RPD / RPM)	Not Vulnerable
VVX 501/601	Vulnerable
All other VVX	Not Vulnerable
Trio (8800, 8500)	Vulnerable
Trio Visual+	Vulnerable
CX Phones (CX5100, CX5500)	Vulnerable
SoundPoint	Not Vulnerable
SoundPoint IP	Not Vulnerable
SoundStation	Not Vulnerable
SoundStation IP	Not Vulnerable
SoundStructure	Not Vulnerable
RealPresence Resource Manager	Vulnerable
RealPresence Collaboration Server / RMX	Vulnerable
RealPresence Access Director	Vulnerable
RealPresence MediaSuite	Vulnerable
RealPresence WebSuite	Vulnerable
VBP	Investigating
RealAccess Cloud Service	Investigating
Polycom Cloud Service	Investigating
RP Touch	Investigating
Polycom Touch Control	Investigating
ISDN Gateway	Not Vulnerable
DMA	Vulnerable
RealConnect for O365	Investigating
VoxBox	Investigating
VoiceStation/VTX	Investigating
SoundStation 2W	Investigating
VVX D60 DECT	Not Vulnerable

CVSS v3 Base Metrics:

To assist our customers in the evaluation of this vulnerability; Polycom leverages 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:

Speculative Execution Vulnerability: 5.6 Medium (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)

For more information on CVSS v3 please see: https://nvd.nist.gov/vuln-metrics/cvss

Severity: Medium

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:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

For the latest information, you may also find value in the security guidance and security news located at:

http://www.polycom.com/security

Note

The below applies to all Polycom security publications:

Polycom may at times issue either a ***Security Advisory*** or a ***Security Bulletin*** with regards to a particular vulnerability or set of vulnerabilities. If a ***Security Advisory*** is issued, this means that one more Polycom products are under investigation or verified by Polycom to be affected by one or more vulnerabilities. If a ***Security Bulletin*** is issued, Polycom is providing its customers with information about one or more vulnerabilities that have not been found by Polycom to directly affect any Polycom products, but that may be mistakenly thought to affect Polycom products. A ***Security Advisory*** might also be issued when a customer's environment might be affected, when false positives might occur from vulnerability scans, or when any other possible (but not actual) concern might exist regarding Polycom products and the vulnerability.

Revision History

Revision 1.0 – Original publication: January 4th, 2018
Revision 1.1 – Updated Summary, Impact and Risk, Mitigations and Notes details: January 5th, 2018
Revision 1.2 – Updated product list: January 9th, 2018
Revision 1.3 – Updated status on several products and increased CVSS score: January 10th, 2018