

SECURITY ADVISORY – Processor based “Speculative Execution” Vulnerabilities AKA “Spectre” and “Meltdown” – Version 1.5

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

DATE PUBLISHED: January 18th, 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”

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.

There are three known variants of the issue:

Variant 1: CVE-2017-5753 - speculative execution bounds-check bypass

Variant 2: CVE-2017-5715 - speculative execution branch target injection

Variant 3: CVE-2017-5754 - speculative execution permission faults handling

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

Many modern CPUs use speculative execution and are potentially susceptible to these types of attacks. However, it is important to note an attacker must be able to execute malicious code on a vulnerable device to exploit one of these vulnerabilities and gain access to restricted memory.

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.

Polycom products are designed and deployed in a manner that largely 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 and the ability to load or execute code is limited to privilege users and firmware signature validation blocks the installation of firmware not signed by Polycom.

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, restricting account access to trusted administrators and disabling shell access.

Customer Mitigations:

- Limit access to critical infrastructure equipment to only trusted administrators from trusted administrative networks or hosts.
- Ensure that all default passwords have been changed.

Polycom will be developing software fixes for supported products found to be vulnerable to prevent these types of attacks. This advisory will be updated as patches are made available.

Products

Product	Variant 1: bounds check bypass (CVE-2017-5753)	Variant 2: branch target injection (CVE-2017-5715)	Variant 3: permission fault handling (CVE-2017-5754)
Group Series	Vulnerable	Vulnerable	Not Vulnerable
Centro	Vulnerable	Vulnerable	Not Vulnerable
Medialign	Vulnerable	Vulnerable	Not Vulnerable
Debut	Vulnerable	Vulnerable	Not Vulnerable
HDX	Not Vulnerable	Not Vulnerable	Not Vulnerable
Pano	Vulnerable	Vulnerable	Not Vulnerable
RealPresence Desktop and Mobile (RPD / RPM)	Not Vulnerable	Not Vulnerable	Not Vulnerable
VVX 501/601	Vulnerable	Vulnerable	Not Vulnerable
All other VVX	Not Vulnerable	Not Vulnerable	Not Vulnerable
Trio (8800, 8500)	Vulnerable	Vulnerable	Not Vulnerable
Trio Visual+	Vulnerable	Vulnerable	Not Vulnerable

CX Phones (CX5100, CX5500)	Vulnerable	Vulnerable	Not Vulnerable
SoundPoint	Not Vulnerable	Not Vulnerable	Not Vulnerable
SoundPoint IP	Not Vulnerable	Not Vulnerable	Not Vulnerable
SoundStation	Not Vulnerable	Not Vulnerable	Not Vulnerable
SoundStation IP	Not Vulnerable	Not Vulnerable	Not Vulnerable
SoundStructure	Not Vulnerable	Not Vulnerable	Not Vulnerable
RealPresence Resource Manager	Vulnerable	Vulnerable	Vulnerable
RealPresence Collaboration Server / RMX	Vulnerable	Vulnerable	Vulnerable
RealPresence Access Director	Vulnerable	Vulnerable	Vulnerable
RealPresence MediaSuite	Vulnerable	Vulnerable	Vulnerable
RealPresence WebSuite	Vulnerable	Vulnerable	Vulnerable
VBP	Investigating	Investigating	Investigating
RealAccess Cloud Service	Not Vulnerable	Not Vulnerable	Not Vulnerable
Polycom Cloud Service	Not Vulnerable	Not Vulnerable	Not Vulnerable
RP Touch	Vulnerable	Vulnerable	Not Vulnerable
Polycom Touch Control	Vulnerable	Vulnerable	Not Vulnerable
ISDN Gateway	Not Vulnerable	Not Vulnerable	Not Vulnerable
DMA	Vulnerable	Vulnerable	Vulnerable
RealConnect for O365	Not Vulnerable	Not Vulnerable	Not Vulnerable
VoxBox	Not Vulnerable	Not Vulnerable	Not Vulnerable
VoiceStation/VTX	Not Vulnerable	Not Vulnerable	Not Vulnerable
SoundStation 2W	Not Vulnerable	Not Vulnerable	Not Vulnerable
VVX D60 DECT	Not Vulnerable	Not Vulnerable	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 revised CVSS score: January 10th, 2018

Revision 1.4 – Updated product status, updated Vulnerability Summary and Mitigations: January 12th, 2018

Revision 1.5 – Updated product status: January 18th, 2018

©2018, Polycom, Inc. All rights reserved.

Trademarks

SECURITY ADVISORY – “SPECTRE” OR “MELTDOWN” – JANUARY 18TH, VERSION 1.5

POLYCOM®, the Polycom logo and all names and marks associated with Polycom and Polycom's products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

Disclaimer

While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical errors, out of date information, or any errors or omissions in the content of this document. Polycom reserves the right to change or update this document at any time. Individuals are solely responsible for verifying that they have and are using the most recent Technical Bulletin.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.