



SECURITY ADVISORY 102522
Advisory Version 1.0 – Initial Release

Advisory Relating to Path Traversal Vulnerabilities in Polycom® VVX® Business Media Phones.

DATE PUBLISHED: December 9th, 2015

This information applies to Polycom VVX 101, 201, 300, 310, 400, 410, 500, 600, and 1500 phones running UC Software versions:

4.1.8 and earlier
5.2.3 and earlier
5.3.1 and earlier
5.4.0 and earlier

Please Note: This is a living document. 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

Polycom VVX phones (all models) are vulnerable to path traversal manipulations that could be used by a malicious party to gain unauthorized access to the system.

Details

Polycom has implemented changes to the UC Software for VVX phones to address these directory traversal vulnerabilities in UCS versions starting with 5.2.4, 5.3.2 and 5.4.0A.

VVX administrators can download one of these non-vulnerable UCS versions (or newer) through this link:

http://support.polycom.com/PolycomService/support/us/support/voice/business_media_phones/

Any customer using an affected phone who is concerned about this vulnerability within their deployment should contact Polycom Technical Support— either call 1-800-POLYCOM or log a ticket online at: <http://support.polycom.com/PolycomService/home/home.htm>

Mitigations

For customers who cannot immediately upgrade to a non-vulnerable UCS version, administrators may mitigate this vulnerability by disabling the web server on VVX phones. In addition, we recommend administrators follow standard best practices and change all default passwords and firewall web access to VVX phones.

To disable a phone's web server via provisioning, set the **httpd.enabled** parameter to **0** in your profiles. Consult the VVX Administrator Guide for additional details. This setting can also be reconfigured directly on the phone by an administrator, under:

Settings -> Advanced -> Administration Settings -> Web Server Configuration.

On Polycom phones with UC Software 5.1.1 or later that are registered with a Skype for Business Server, access to the Web Configuration Utility is by default disabled as a security precaution.

CVSS v2 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 v2 Scores:

5.8 (AV:A/AC:M/Au:S/C:C/I:P/A:N)

For more information on CVSS v2 please see:

<http://www.first.org/cvss/cvss-guide.html>

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.

Acknowledgement

This vulnerability was first discovered and brought to Polycom's attention by Jake Reynolds of Depth Security (www.depthsecurity.com). We would like to thank Mr. Reynolds and Depth Security for their coordinated disclosure of these vulnerabilities.

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

<http://www.polycom.com/security>

Revision History

Revision 1.0 - Original publication: December 9th, 2015 – First Announcement

©2015, Polycom, Inc. All rights reserved.

Trademarks

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 Advisory.

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.

