



SECURITY BULLETIN – WannaCry – CVE-2017-0146 and CVE-2017-0147 – Bulletin
Version 1.1

Security Bulletin Relating to *CVE-2017-0146 and CVE-2017-0147* “WannaCry” Vulnerability and Polycom Products

DATE PUBLISHED: August 10th, 2017

This information applies to the WannaCry (also called WannaCrypt, WanaCrypt0r 2.0, and Wanna Decryptor) vulnerability and Polycom products. This document is an information bulletin and thus does not contain a table of Polycom products and versions. This omission is intentional, as there is no known WannaCry vulnerability in any current Polycom product at this time. Legacy Polycom products that are outside of their support window have not been evaluated for potential vulnerabilities.

Any information in this bulletin is subject to change.

Please Note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this bulletin has been repaired against that vulnerability. 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

The WannaCry ransomware takes advantage of flaws in Microsoft’s implementation of the SMBv1 protocol. Polycom’s currently released appliances and endpoints are not vulnerable to WannCrypt because they use a variant of Linux or Android.

Polycom has a legacy provisioning and management server called CMA which was Windows-based. Customers with the CMA may wish to transition from their existing CMA by upgrading to Polycom’s RealPresence Resource Manager to avoid the potential for WannaCry.

Vulnerability Details

CVE-2017-0146

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0146>

“The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148”

And

CVE-2017-0147

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147>

“The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability.”

Impact and Risk

There is no risk from WannaCry in current Polycom appliances and endpoints.

Polycom has several software applications, such as the RealPresence Desktop soft client, that runs on Windows-based computer systems, and while such applications are not vulnerable, the workstation on which the application is installed may be vulnerable. Polycom recommends that customers follow the guidance suggested by Microsoft in their security notice for patching and securing their computer systems against the WannaCry and other vulnerabilities.

Solution

Polycom’s currently released products are not vulnerable to the WannaCry vulnerability reported in CVE-2017-0146 and CVE-2017-0147, and therefore, no actions are required.

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:

CVE-2017-0146: 8.1 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2017-0147: 5.9 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

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

Severity: Critical

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 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: May 16th, 2017

Revision 1.1 – Updated verbiage for clarity based on customer feedback: August 10th, 2017

©2017, 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 SECURITY ADVISORY OR SECURITY 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.

