SECURITY ADVISORY – “BlueBorne” Bluetooth Vulnerabilities – Advisory Version 1.0

Security Advisory Relating to BlueBorne Attack Vectors and Polycom Products: *CVE-2017-1000250* and *CVE-2017-1000251*

DATE PUBLISHED: September 25th, 2017

This information applies to BlueBorne vulnerabilities and how they might apply to Polycom products that use Bluetooth. Polycom is conducting ongoing research to determine the level of vulnerability (if any) for each of its various products.

Any information in this advisory is subject to change.

Please Note: This is a living document, updated regularly until any product affected by any of the vulnerabilities in this advisory 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

Products that support Bluetooth technology may be susceptible to a set of attack vectors, collectively named the BlueBorne vulnerabilities. Polycom is investigating all products that support Bluetooth for exposure to theses vulnerabilities and will update this advisory as information becomes available.

Vulnerability Details

CVE-2017-1000251

The BlueZ Bluetooth stack in the Linux Kernel, starting with Linux kernel version 3.3-rc1 up to and including kernel 4.13.1, is vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote Code Execution in kernel space.

And

CVE-2017-1000250

All versions of the SDP server in BlueZ 5.46 and earlier are vulnerable to an information disclosure vulnerability which allows remote attackers to obtain sensitive information from the bluetoothd process memory. A specially crafted Bluetooth device could, without prior pairing or user interaction, retrieve portions of the bluetoothd process memory, including potentially sensitive information such as Bluetooth encryption keys.

Products Under Investigation

Note: The below table is limited to Polycom products with Bluetooth functionality. All products not listed have been determined to operate without Bluetooth capabilities and are deemed to not be vulnerable.

Polycom VVX (600 and 601)	Investigating
Polycom Trio (all models)	Investigating
Polycom Pano	Not Vulnerable
Polycom VoxBox	Not Vulnerable

Impact and Risk

We are continuing to investigate whether BlueBorne impacts Polycom Trio and VVX phones, but it has not yet been concluded that any Polycom products are affected at the publication time of this bulletin.

Mitigations

Polycom recommends that concerned customers disable Bluetooth capabilities on their devices. Please consult the Administrator's Guide for your specific product for detailed instructions to configure Bluetooth.

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.

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

Base CVSS v3 Scores:

CVE-2017-1000251: 7.5 (CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

Severity: High

CVE-2017-1000250: 6.5 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

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:

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

Note:

Effective January 1, 2014, 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 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: September 25th, 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 Technical Bulletin or 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.