SECURITY ADVISORY – "GHOST" (*glibc* Vulnerability CVE-2015-0235)
Advisory Version 2.0 - Final

Security Advisory Relating to "GHOST" *glibc* Vulnerability on Various Polycom Products.

DATE PUBLISHED: October 23rd, 2015

This information would apply only to all Polycom products that incorporate the Linux *glibc* library. 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

A vulnerability has been recently disclosed in the glibc gethostbyname() function used by some Linuxand Linux-based operating systems. This vulnerability could potentially allow an attacker to inject code into a process that calls the vulnerable function. The vulnerability is known as GHOST and has been assigned the following CVE identifier:

CVE-2015-0235: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235

Details

CVE-2015-0235, aka "GHOST"

A heap-based buffer overflow was found in the __nss_hostname_digits_dots function of glibc 2.2, and other 2.x versions before 2.18, which is used by the gethostbyname() and gethostbyname2() glibc function calls. A remote attacker could potentially inject code into a process that calls the vulnerable functions to execute arbitrary code.

Mitigations

Although there may be multiple attack vectors by which this vulnerability can be exploited, it seems to be fairly challenging to exploit. Polycom products do not make typical use of the most likely vectors of attack: MTAs, web-reachable diagnostic tools, or client applications such as web browsers.

Exploitation of this glibc vulnerability would require that a program on your Polycom device performs a lookup of a host name provided by an attacker via a compromised DNS server. The lookup would need to be done in a very particular manner and must lack some commonly-employed sanity checks. Further, gethostbyname() functions have been obsoleted within IPv6-supported applications by way of the getaddrinfo() call. We are continuing to investigate whether this completely mitigates the impact of this vulnerability on certain Polycom devices.

An effective mitigation strategy will incorporate techniques both from within the product and within the deployment architecture. Steps that may be taken include, but are not limited to: Protect your systems from corrupted outside servers via network firewalling or separation. Protect your systems from unauthorized access with named accounts and complex passwords. Use firewalls or VLAN's to limit scope of name lookups. Use IP addresses rather than names where possible. Use IPv6 where possible.

Products Affected

Note that the products listed in the below table are the only products whose vulnerability status can be definitively stated at this time – to the positive or the negative. Any products not listed in this chart remain under investigation, and will appear in this chart as soon as their status is known.

Media Manager – All Versions	Not Vulnerable
CMAD (CMA Desktop) – All Versions	Not Vulnerable
CX5000 – All Versions	Not Vulnerable
Video Border Proxy (VBP) – All Versions	FIXED – version 11.2.22
CX Product Line, All Other Video Versions	Not Vulnerable
RealPresence Desktop – All Versions	Not Vulnerable
Group Series – All Versions	Not Vulnerable
Capture Station – All Versions	Not Vulnerable
RealPresence Access Director (RPAD) – All Versions	Not Vulnerable
CloudAXIS MEA – All Versions	Not Vulnerable
CloudAXIS WSP – All Versions	FIXED – version 1.7.0
Platform Director – All Versions	FIXED – version 2.0
HDX – All Versions	FIXED – version 3.1.7
RealPresence Resource Manager (RPRM)	FIXED – version 8.3.1
RSS 4000 – All Versions	FIXED – version 8.5.3
Distributed Media Application (DMA) – All Versions	FIXED – version 6.2.1 and 6.1.3
Capture Server	FIXED – version 2.0
Content Sharing Suite Client/Server – All Versions	FIXED – version 1.5
RealPresence Collaboration Server (RMX) – All Versions	FIXED – 8.4.2 Hotfix available from

	support
RealPresence Mobile – All Versions	Not Vulnerable
UC Phones – VVX - All Versions	FIXED – UCS 5.3
UC Phones – SPIP & SSIP – All Versions	Not Vulnerable

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:

CVE-2015-0235: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

For more information on CVSS v2 please see:
http://www.first.org/cvss/cvss-guide.html

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: January 29, 2015 – First Announcement

Revision 1.1 - Unpublished

Revision 1.2 – Second publication: February 4, 2015 – New Products Added

Revision 1.3 – Third publication: February 24, 2015 – Many Products Added; Some Edits

Revision 1.4 – RPAD returned to NOT VULNERABLE, better detail on phones

Revision 1.5 – Updated fix and release information

Revision 1.6 – Updated fix and release information

Revision 1.7 – Updated fix and release information

Revision 1.8 – Updated fix and release information

Revision 1.9 – Updated fix and release information

Revision 2.0 Final – Updated fixed status on all products

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.