SECURITY ADVISORY – *GNU glibc* DNS Vulnerability (CVE-2015-7547)
Advisory Version 1.2

Security Advisory Relating to a *GNU glibc* DNS Vulnerability in Various Polycom Products

DATE PUBLISHED: April 6th, 2016

This information will apply only to Polycom products that incorporate version 2.9 to 2.23 of the GNU *glibc* library. Polycom is conducting ongoing research to determine the level of vulnerability (if any) for each of our various products.

Any information in this advisory is subject to change.

Please Note: This is a living document, and will be updated regularly until any product affected by 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 libresolv library in the GNU C Library (aka glibc or libc6) between versions 2.9 and 2.23. This vulnerability could potentially allow a remote attacker to create a specially crafted DNS response which could cause libresolv to crash causing a possible denial of service or, potentially, execute code with the permissions of the user running the library. The vulnerability has been assigned a CVE identifier:

CVE-2015-7547: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547

Details

CVE-2015-7547

Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) between versions 2.9 and 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing dual A/AAAA DNS queries. Note: this issue is only exposed when libresolv is called from the nss_dns NSS service module.

Mitigations

An effective mitigation strategy will incorporate techniques both within the product configuration and in the deployment architecture. Polycom recommends additional network and architectural mitigations in all cases, including (but not limited to): Configure your Polycom products to use trusted DNS resolvers. Use IP addresses rather than names where possible. Protect your systems from corrupted outside DNS servers or addresses via network firewalling and separation to limit or block untrusted DNS lookups from Polycom devices. Protect your Polycom systems from unauthorized access with named accounts, complex passwords and by controlling network access to administrative functions.

The vulnerability relies on an oversized (2048+ bytes) UDP or TCP DNS response, which is followed by another response that will overwrite the stack. An effective mitigation would be to limit the response sizes accepted by the DNS resolver called upon by your Polycom devices (*e.g.*, via DNSMasq or similar software deployed locally on the resolver).

In a default libresolv configuration, the UDP-based vector will be mitigated by using a trusted, protocol-compliant DNS resolver on a trusted network. A compliant resolver will not produce the kind of oversized responses which are necessary to exploit this vulnerability. By default, the glibc resolver does not enable EDNS0 and does not request large responses. Ensure that DNS queries are sent only to DNS servers which limit the response size for UDP responses with the truncation bit set.

The buffer size configuration option offered by most resolvers only applies to UDP not TCP. The TCP-based vector can be mitigated by using a trusted recursive resolver on a trusted network, if you limit the size of individual DNS responses to 1023 bytes, however we recognize this is non-standard.

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. Any products not listed in this chart remain under investigation, and will appear in this chart as soon as their status is known.

Capture Station – All Versions	Not Vulnerable
Media Manager – All Versions	Not Vulnerable
CMAD (CMA Desktop) – All Versions	Not Vulnerable
CX5000 – All Versions	Not Vulnerable
CX Product Line, All Other Video Versions	Not Vulnerable
Group Series – All Models, All Versions	Not Vulnerable
HDX – All Models, All Versions	Not Vulnerable
RealPresence Desktop – All Versions	Not Vulnerable
RealPresence Mobile – All Versions	Not Vulnerable
UC Phones – SPIP & SSIP – All Models, All Versions	Not Vulnerable
RealPresence Debut – All Versions	Not Vulnerable
VBP – 200 E, 43xx, 4555, 5300-E/ST, 6400-ST	Not Vulnerable
VBP 7301 Series	FIXED – version 14.2.5
Distributed Media Application (DMA) – All Versions	FIXED – version 6.3.2
RealPresence Access Director (RPAD) – All Versions	FIXED – version 4.2.3
Platform Director – All Versions	FIXED – version 3.0

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: February 23, 2015 – First Announcement
Revision 1.1 – Second publication: February 25, 2015 – New Products Added
Revision 1.2 – Third publication: April 6, 2015 – New Products Added