SECURITY BULLETIN – SSLv3 “POODLE” – Bulletin Version 1.6

Security Bulletin Relating to *SSLv3 “POODLE”* Vulnerability and Polycom Products

DATE PUBLISHED: April 20th, 2015

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.

This information applies to products that use SSLv3 clients (such as web browsers). SSLv3 servers are not at risk to POODLE, though they can in theory contribute to client-side exploitation. There are no demonstrated exploits of Polycom SSLv3 servers at this time. 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 POODLE vulnerability in any Polycom system at this time.

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

A vulnerability was discovered in the SSLv3 protocol. Two systems engaged in a dialogue to determine their mutual level of protocol support (TLS included) can often negotiate downward to the older and obsolete SSLv3 protocol during the “handshake” if configurations allow. This vulnerability leverages this phenomenon as well as weaknesses in the CBC padding in SSLv3 to facilitate the establishment of a man-in-the-middle attack whose purpose is to decrypt the dialogue in order to read data in cleartext.

Vulnerability Details

CVE-2014-3566, aka “POODLE”

The SSL protocol version 3.0 (incorporated in OpenSSL through 1.0.1i, and other cryptography products) uses nondeterministic padding for its CBC (“cipher block chaining” encryption), which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. By combining this fact with the downward negotiation described above, a client can be compromised by a malicious server.

“POODLE” is a client vulnerability. Servers (or products with embedded servers in them) that support SSLv3 in theory can contribute somewhat to a client exploitation if the client is not itself properly configured (to disable SSLv3 support) and if other network conditions *and an attacker* are also present. Network conditions are listed in “Impact and Risk” below. Also please see “General Mitigations” for ways to reduce client risk.

Impact and Risk

As of the time of this bulletin’s publication (v1.0), no known exploits of this vulnerability have been reported.

Though this issue has received rapid attention in today’s climate (awareness in the press of security issues has been quite high since Heartbleed), this issue is not a significant threat if the vectors and complexity of attack are understood.

The vulnerability affects SSL clients who encounter a malicious server and who are configured to allow support for the known-vulnerable SSLv3 protocol.

For the CBC mechanism in SSLv3 to be exploited, several factors must exist:

1. The user’s client (generally a web browser) must be set to allow SSLv3 support
2. The user must voluntarily interact with the attack mechanism via social engineering or genuine ignorance of the threat
3. Attacker must be on the same, un-switched network as the user (this rules out nearly all enterprise networks)
4. Attacker must then also successfully spoof a server, create a proxy, or create a conventional man-in-the-middle server. The network environment must permit the deployment of such illegitimate servers.

General Mitigations

Turn off your web browser’s support for SSLv3. Use only TLS v1.2 and TLS v1.1 (or TLS v1.0 if backwards compatibility is required). This is a configurable setting in most modern browsers.

Products Affected

At this point, all Polycom products that contain SSLv3 appear to support SSLv3 only on the server side. All evidence at the time of this bulletin indicates that these products are therefore not at risk themselves. Polycom will be removing SSLv3 support anyway per “Vulnerability Details” above to address any concerns from analysis efforts that only look for the presence of SSLv3 and not its role in the client/server model.

Solution

All Polycom product teams who support SSLv3 are committed to removing that support in the first half of 2015. These products use SSLv3 on the server side, so they are not in themselves vulnerable. As of the date of this bulletin, no Polycom product has been found to be 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-2014-3566: 4.3 (Out of 10.0) (AV:N/AC:M/Au:N/C:P/I:N/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.

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: October 15, 2014

Revision 1.1 – Date commitments, clarification of vulnerability (client vs. server)

Revision 1.2 – Updated fix and commitment dates with some remediations

Revision 1.3 – Better clarity on lack of vulnerability, adjusted date for SSLv3 removal

Revision 1.4 – Updated fix and commitment dates

Revision 1.5 – Updated verbiage

Revision 1.6 – Updated dates and slight format change
