Security Bulletin Relating to **CVE-2016-0800 “DROWN”** Vulnerability and Polycom Products

DATE PUBLISHED: March 8th, 2016

This information applies to products that use SSLv2 which do not include any current Polycom products. There are no demonstrated exploits of DROWN against Polycom products 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 DROWN 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

Products that support SSLv2 could be subject to a vulnerability known as DROWN. This vulnerability has been designated CVE-2016-0800. Used in conjunction with export strength ciphers, SSLv2 can be more easily decrypted by malicious third parties and OpenSSL.org is recommending that SSLv2 be disabled in affected products. The latest version of OpenSSL will do this by default.

Vulnerability Details

**CVE-2016-0800, aka “DROWN”**

The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.
Impact and Risk

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

Solution

No current Polycom products support SSLv2 and are not at risk to this vulnerability.

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-2016-0800: 4.3 (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: TBD

<table>
<thead>
<tr>
<th>Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.</td>
</tr>
<tr>
<td>High</td>
<td>A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.</td>
</tr>
<tr>
<td>Medium</td>
<td>A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.</td>
</tr>
<tr>
<td>Low</td>
<td>A vulnerability that has minimal impact to the system and is extremely difficult to exploit.</td>
</tr>
</tbody>
</table>
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: March 8th, 2016
document at any time. Individuals are solely responsible for verifying that they have and are using the most recent Technical 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.