



SECURITY BULLETIN CVE-2014-0160 Version 1.9

---

## Security Advisory Relating to OpenSSL Vulnerability “Heartbleed” on Various Polycom Products

DATE PUBLISHED: 2014-04-28-13:19 CDT (UTC -5)

**This information applies to all Polycom products using OpenSSL versions 1.0.1 through 1.0.1f.**

---

***Please remember that this bulletin is being updated on a regular basis to address new information regarding vulnerabilities and new fixes. This bulletin is versioned and time stamped. The newest version will always be located at this URL:***

***<http://www.polycom.com/content/dam/polycom/common/documents/brochures/heartbleed-security-advisory-enus.pdf>***

---

### **Vulnerability Summary**

*A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.*

### **Details**

*Through exploiting the heartbeat feature in OpenSSL versions 1.0.1 through 1.0.1f, an attacker can capture memory from the host 64k at a time. Successive 64k sections of memory can be captured until the attacker has captured the desired data. This could include, at worst case, a copy of the server's private key.*

*This exploit is consistent with CVE: 2014-0160*

## Systems Affected

At this time, a list of Polycom products, their versions, and vulnerability status is outlined in the table below. This bulletin will be updated periodically until all known vulnerable Polycom systems are fixed or properly mitigated. **NOTE: Any dates listed in the table below are ESTIMATES. These dates are subject to change, for better or worse, as new information becomes available to the teams in charge of each product. Vulnerability status may be subject to change pending new information.**

### Comprehensive Vulnerability Assessment of Polycom Products (4 Parts)

| Product Name   | Version                  | Vulnerable        | Notes and/or FIX/FIXED Dates  |
|--|--------------------------|-------------------|---|
| <b>Management Applications</b>                         |                          |                   |   |
| CMA  | All                      | Not Vulnerable    |   |
| RealPresence Distributed Media Application (DMA)       | All                      | Not Vulnerable    |   |
| RealPresence Resource Manager (RPRM)                   | All                      | Not Vulnerable    |   |
| RealPresence Video DualManager 400 (RPDM)              | All                      | Not Vulnerable    |   |
| RealPresence Platform Suite (SoftRPP)                  | All                      | Not Vulnerable    |   |
| <b>Telepresence Rooms</b>                              |                          |                   |   |
| VSX Series   | All                      | Not Vulnerable    |   |
| <b>HDX Series</b>                                      |                          |                   |   |
| HDX  | 2.7.0.x - 3.0.x          | Not Vulnerable    |   |
| <b>HDX</b>   | <b>3.1.x and Greater</b> | <b>Vulnerable</b> | <b>FIXED in version 3.1.3.2</b>   |
|  |                          |                   | Fixes Earlier 3.x Vulnerable Versions - <b>NOT currently recommended for CMS/Halo</b>                           |
| HDX  | 3.1.3.2                  | Not Vulnerable    |   |
| QDX 6000   | All                      | Not Vulnerable    |   |
|  |                          |                   | <b>See below. 4.1.3.2 fixes all 4.1 versions. 4.0.2.2 will fix all 4.0 versions w/ estimated date of May 15</b> |
| <b>RealPresence Group Series</b>                       | <b>All Versions</b>      | <b>Vulnerable</b> |   |
| RealPresence Group Series                              | 4.1.3.2                  | Not Vulnerable    | Fixes all 4.1 versions  |
| <b>Unified Conference &amp; Collaboration Stations</b> |                          |                   |   |
| CX5000, CX5100, CX5500, CX7000, CX8000                 | All                      | Not Vulnerable    |   |



| Product Name  | Version                    | Vulnerable        | Notes and/or FIX/FIXED Dates   |
|---|----------------------------|-------------------|--|
| <b>Immersive Telepresence</b>   |                            |                   |  |
| ITP with HDX (ATX, OTX, RPX, TPX) - See HDX Section for Any Fixes                 |                            |                   |  |
| ITP   | 2.7.1                      | Not Vulnerable    | Uses HDX 2.6.1.3_itp271-5267   |
| ITP   | 3.0.1                      | Not Vulnerable    | Uses HDX 3.0.1-10628   |
| ITP   | 3.0.2                      | Not Vulnerable    | Uses HDX 3.0.2-11176   |
| ITP   | 3.0.3                      | Not Vulnerable    | Uses HDX 3.0.3-14451   |
| ITP   | 3.0.5                      | Not Vulnerable    | Uses HDX 3.0.5-22695   |
| <b>ITP</b>  | <b>3.1</b>                 | <b>Vulnerable</b> | <b>3.1.3.2 Fixes vulnerability</b>                                     |
| <b>ITP</b>  | <b>3.1.2</b>               | <b>Vulnerable</b> | <b>3.1.3.2 Fixes vulnerability</b>                                     |
| <b>ITP</b>  | <b>3.1.3</b>               | <b>Vulnerable</b> | <b>3.1.3.2 Fixes vulnerability</b>                                     |
| ITP with Group Series (Immersive Studio) - See Group Series Section for Any Fixes |                            |                   |  |
| <b>RPIS</b>   | <b>4.1.2</b>               | <b>Vulnerable</b> | <b>Uses Group Series 4.1.2-100236</b>                                  |
| <b>RPIS</b>   | <b>4.1.3</b>               | <b>Vulnerable</b> | <b>Uses Group Series 4.1.3-111080</b>                                  |
| <b>CMS/Halo</b>   | <b>All</b>                 | <b>Vulnerable</b> | <b>HDX and RMX are the only vulnerable components.</b>                 |
| <b>Desktop &amp; Mobile Video Conferencing</b>                                    |                            |                   |  |
| RealPresence Desktop  | All Versions               | Not Vulnerable    |  |
| RealPresence Mobile   | All Versions               | Not Vulnerable    |  |
| CMA Desktop   | All Versions               | Not Vulnerable    |  |
| <b>Collaboration Servers</b>  |                            |                   |  |
| RealPresence Collaboration Server 1500, 1800, 2000 and 4000 (RMX)                 |                            |                   |  |
| RMX   | 7.5.x - 7.8.x              | Not Vulnerable    |  |
| <b>RMX</b>  | <b>8.1.4.J</b>             | <b>Vulnerable</b> | <b>Fixes pending</b>   |
| <b>RMX</b>  | <b>8.1.4.x</b>             | <b>Vulnerable</b> | <b>Fixes pending</b>   |
| <b>RMX</b>  | <b>8.1.7.x</b>             | <b>Vulnerable</b> | <b>Fixes pending</b>   |
| <b>RMX</b>  | <b>8.2.x</b>               | <b>Vulnerable</b> | <b>8.2.0.85.0.13.544.002 will fix. Estimated delivery of April 28.</b> |
| <b>RMX</b>  | <b>8.3.x</b>               | <b>Vulnerable</b> | <b>Fixed with Hotfix 8.3.0.245.477.003</b>                             |
| RMX   | 8.3.0.245.477.003 (Hotfix) | Not Vulnerable    | Fixes 8.3.x  |
| MGC-25, MGC-50, MGC-100   | All                        | Not Vulnerable    |  |
| RealPresence Collaboration Server, Virtual Edition (SoftMC)                       | 8.3.x                      | Not Vulnerable    |  |
| S4GW Serial Gateway for RMX   | All                        | Not Vulnerable    |  |

| Product Name                              | Version             | Vulnerable        | Notes and/or FIX/FIXED Dates      |
|---|---------------------|-------------------|-----------------------------------|
| <b>Media Capture &amp; Sharing</b>        |                     |                   |                                   |
| Recording and Streaming Server (RSS) 4000 | All Versions        | Not Vulnerable    |                                   |
| Recording and Streaming Server (RSS) 2000 | All Versions        | Not Vulnerable    |                                   |
| RealPresence Capture Server               | All Versions        | Not Vulnerable    |                                   |
| RealPresence Capture Station Pro          | All                 | Not Vulnerable    |                                   |
| RealPresence Capture Station Portable Pro | All                 | Not Vulnerable    |                                   |
| RealPresence Media Manager                | All                 | Not Vulnerable    |                                   |
| Media Editor                              | All                 | Not Vulnerable    |                                   |
| CSS Client                                | All Versions        | Not Vulnerable    |                                   |
| CSS Server                                | All Versions        | Not Vulnerable    |                                   |
| <b>Firewall Traversal &amp; Security</b>  |                     |                   |                                   |
| Video Border Proxy (VBP) E & ST Series    |                     |                   |                                   |
| VBP                                       | 11.1.x              | Not Vulnerable    |                                   |
| VBP                                       | 11.2.11 - Hotfix    | Not Vulnerable    |                                   |
| <b>VBP</b>                                | <b>11.2.12 - GA</b> | <b>Vulnerable</b> | <b>FIXED with version 11.2.17</b> |
| <b>VBP</b>                                | <b>11.2.16 - GA</b> | <b>Vulnerable</b> | <b>FIXED with version 11.2.17</b> |
| VBP                                       | 11.2.17             | Not Vulnerable    | Fixes Earlier Vulnerable Versions |
| RealPresence Access Director (RPAD)       | All Versions        | Not Vulnerable    |                                   |
| <b>CloudAXIS</b>                          |                     |                   |                                   |
| CloudAXIS MEA (Web experience portal)     | All Versions        | Not Vulnerable    |                                   |
| CloudAXIS WSP (Web service portal)        | All Versions        | Not Vulnerable    |                                   |
| RealPresence Platform Director            | All Versions        | Not Vulnerable    |                                   |

| Product Name  | Version   | Vulnerable        | Notes and/or FIX/FIXED Dates   |
|---|---|-------------------|--|
| <b>Desktop Video &amp; Voice Solutions</b>                                    |   |                   |  |
| Soundpoint, Soundstation, SoundStructure, VVX                                 |   |                   |  |
| SoundPoint, SoundStation, VVX and SoundStructure (VoIP Interface) Families    | UCS 4.0.1.13681 rts56 -<br>UCS 4.0.5.4233 rts22           | Not Vulnerable    |  |
| SoundPoint, SoundStation, VVX Families  | UCS 3.3.0.1098 rts35 -<br>UCS 3.3.4.0085 rts6             | Not Vulnerable    |  |
| SoundPoint, SoundStation, VVX Families  | SIP 3.2.0 rts44 -<br>SIP 3.2.7.0198 rts10                 | Not Vulnerable    |  |
| <b>SoundPoint, SoundStation, and SoundStructure (VoIP Interface) Families</b> | <b>UCS 4.1.0.84959 rts42 I -<br/>UCS 4.1.6.4835 rts50</b> | <b>Vulnerable</b> | <b>UCS 4.1.6 patch FIX delivered; UCS 5.0.2 patch FIX delivered; UCS 4.1.0 patch FIX delivered; <u>UCS 5.1.0 patch due May 6; UCS 4.1.7 patch due May 13</u></b> |
| <b>VVX and SoundStructure (VoIP Interface) Families</b>                       | <b>UCS 4.1.3.7864 rts21G -<br/>UCS 5.0.1.7396 rts56 Q</b> | <b>Vulnerable</b> | <b>UCS 4.1.6 patch FIX delivered; UCS 5.0.2 patch FIX delivered; UCS 4.1.0 patch FIX delivered; <u>UCS 5.1.0 patch due May 6; UCS 4.1.7 patch due May 13</u></b> |
| Zero Touch Provisioning Solution - ZTP (User Portal)                          | N/A   | Not Vulnerable    | FIXED as of April 11, 2014   |
| <b>Unified Conference &amp; Collaboration Stations</b>                        |   |                   |  |
| CX100, CX300, CX500, CX600, CX3000  | All   | Not Vulnerable    |  |
| <b>Accessories</b>  |   |                   |  |
| TouchControl (PTC)  | All   | Not Vulnerable    |  |
| People + Content IP (PPCIP)   | All   | Not Vulnerable    |  |

## Mitigation

At this time, many affected products have older versions to which you can temporarily regress (install older version). If you can temporarily run an older product version, this is recommended.

For some products, mitigations exist solely in the realm of controlling the presence of encrypted traffic on any system that uses a vulnerable version of OpenSSL. Basic suggestions at this time are to:

1. Place the Polycom product behind a firewall whenever possible, such that outsiders do not have access to ports used by OpenSSL on the device (usually only HTTPS, but sometimes other protocols that use TLS such as secure LDAP or secure SIP are involved).
2. Turn off any services that use OpenSSL (if relevant) if at all possible. When new fixes become available, new certificates can be issued for your system, thus occluding any knowledge an attacker might have gained with regards to your old encryption certificates or keys.

**For the voice products currently listed as vulnerable, a mitigation specific to these products is available: Set your http.enabled flag to = 0 (zero). This disables web access of all kinds, and blocks known heartbeat vectors into the system.**

Note that Polycom's Product Security Office is working rapidly and efficiently to assist product teams in delivering fixes in as rapid a manner as possible.

## Solution

As fixes become available for a given product, that information will appear in this bulletin in subsequent releases. Polycom will continue updating this bulletin until all fixes are in place. Polycom recommends that users of any Polycom



product listed in the table above as being vulnerable update to the “FIXED” version of their product as soon as such a version becomes available.

### 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 Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

| Access Vector  | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
|----------------|-------------------|----------------|------------------------|------------------|---------------------|
| <b>Network</b> | <b>Low</b>        | <b>None</b>    | <b>Partial</b>         | <b>None</b>      | <b>None</b>         |

## Severity: High

| Rating          | Definition   |
|-----------------|--|
| <b>Critical</b> | A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.  |
| <b>High</b>     | A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources. |
| <b>Medium</b>   | A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.                      |
| <b>Low</b>      | 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](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>

---

**Please remember that this bulletin is being updated on a regular basis to address new information regarding vulnerabilities and new fixes. This bulletin is versioned and time stamped. The newest version will always be located at this URL:**

<http://www.polycom.com/content/dam/polycom/common/documents/brochures/heartbleed-security-advisory-enus.pdf>

---

## Acknowledgment

Polycom discovered this vulnerability through the CVE database.



**Revision History – Security Bulletin CVE-2014-0160**

|             |                  |  |
|-------------|------------------|--|
| Version 1.0 | 2014-04-09-15:20 | Initial release with 90% complete list of products and their vulnerability status  |
| Version 1.1 | 2014-04-10-20:00 | More detail for more products and first estimates for fix dates. Improved mitigation detail.   |
| Version 1.2 | 2014-04-14-12:21 | More products, better detail, better listings for affected members of Soundpoint family  |
| Version 1.3 | 2014-04-14-21:17 | Product list condensation (“versions older than”). HDX and Group Series fix date estimates published. Incorrect mitigation advice for RMX posted.  |
| Version 1.4 | 2014-04-15-07:24 | More condensation and accuracy. Mitigation advice removed from RMX.  |
| Version 1.5 | 2014-04-17-12:38 | RMX estimate for fix date, HDX fix date estimate moved in, mitigation for those members of Soundpoint family affected  |
| Version 1.6 | 2014-04-18-10:27 | Added UCS fix dates for the affected VVX, Soundstation, Soundstructure systems. Added new language at the top and bottom of the document reminding that it is a living doc, updates of which can be found on Polycom’s website |
| Version 1.7 | 2014-04-22-21:47 | New formatting, fix announcements for HDX and RMX, condensed table format  |
| Version 1.8 | 2014-04-26-06:07 | Group Series fix announced. More detail for RMX fixes for older versions. Added PPCIP. Note about ITP and HDX fix. Changed dates on UCS phones.  |
| Version 1.9 |                  | Clarification on HDX/ITP and HDX/CMS, Fixes for many of the UCS phones, CMS/Halo & S4GW added as their own items.  |



©2013, 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.

**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.

