Security Alert Relating to TLS 1.2 and Microsoft O365

DATE PUBLISHED: July 5th, 2018

This information applies to Polycom products and changes with Microsoft's O365 support for TLS 1.0 and 1.1 and for customers who wish to update to TLS 1.2. Polycom is continuing to investigate the impact to our product lines to determine which products may be affected by this change.

Any information in this Alert is subject to change as our investigation progresses.

Please Note: This is a living document, and Polycom will update this advisory regularly as the investigation progresses and new information becomes available. 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

Change Summary

Microsoft O365 Will Stop Support for TLS 1.0 and 1.1 in October of 2018

On October 31st, 2018, Microsoft Office 365 will no longer support the use of TLS 1.0 or 1.1 for communications. Once Office 365 deprecates support for these protocols, all communications to and from Office 365 servers will need to use TLS 1.2 and Polycom CX600, CX3000 and CX8000 will no longer connect or be supported.

Devices will not register to any Skype for Business server if TLS is updated to TLS 1.2

If upgrading to TLS 1.2 using Skype for Business Servers (on-premises), the additional devices listed below will no longer be able to register to Skype for Business or be supported. Compliance requirements such as Payment Card Industry Date Security Standard (PCI-DSS) will require that customers implement a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) by June 30th 2018 in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact and Risk

Polycom is investigating and will continue to investigate all products and product lines to determine if there will be an impact. At this time, it is known that the following products will be impacted by this change in support:

- Polycom CX500 phone
- Polycom CX600 phone
- Polycom CX700 phone
- Polycom CX3000 conference phone
- Polycom CX8000 Skype Room System

Mitigations

If using these products, continue to use them with Skype for Business Server 2015 (on-premises) without updating to TLS 1.2

Microsoft Links: **Deprecating support for TLS 1.0 and 1.1**

https://support.office.com/en-us/article/technical-reference-details-about-encryption-in-office-365-862cbe93-4268-4ef9-ba79-277545ecf221

https://support.microsoft.com/en-us/help/4057306/preparing-for-tls-1-2-in-office-365

https://techcommunity.microsoft.com/t5/Skype-for-Business-Blog/Certified-Skype-for-Business-Online-Phones-and-what-this-means/ba-p/120035

Polycom Links:

http://www.polycom.com/collaboration-solutions/microsoft-unified-communications/microsoft-teams.html

Other Links:

http://tomtalks.uk/2018/03/office-365-will-enforce-mandatory-use-of-tls-1-2-from-october-31-2018-and-lync-phone-edition-doesnt-support-tls-1-2-so/

https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls

Contact

Any customer using an affected system who is concerned about this change 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 may also find value in the security guidance and security news located at:

http://www.polycom.com/security

Note

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 under investigation or 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: July 5th, 2018

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.