平成 29 年 11 月 29 日

お客様各位

株式会社プリンストン

セキュリティ勧告：Polycom HDX に対する遠隔地からのコード実行の脆弱性

平素は格別のご高配を賜り厚く御礼申し上げます。

平成 29 年 11 月 15 日にポリコム社から Polycom HDX の脆弱性に関する情報が公開されました。本書はポリコム社の勧告原文(英語)及び弊社で日本語に翻訳したものと合わせて対応方法等を記載したものです。英語と日本語の翻訳に差異がある場合は、原文(英語)を優先します。
対象機器がある場合は、以下の「解決策」または「緩和策」を実施していただくことを強く推奨いたします。

以下、原文(英語)

Security Advisory Relating to Remote Code Execution Vulnerability on Polycom HDX Endpoints

DATE PUBLISHED: November 15, 2017

Any information in this advisory is subject to change.

Please note: 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 critical vulnerability has been discovered in the Polycom shell (psh) functionality on the HDX's diagnostics port (port tcp/23). This vulnerability could allow a remote attacker to execute arbitrary code on the HDX, which could lead to compromise of the system.

Products Affected

HDX 3.1.11 hotfix 1 and earlier	Fixed in HDX 3.1.11 hotfix 2 or later

Solution

Update to HDX 3.1.11 hotfix 2 or later, available at the Polycom Support web site:

http://support.polycom.com/content/support/North_America/USA/en/support/video/hdx_series.html

In the event that your organization requires Generally Available or "GA" release software, we expect this software will be made available in the coming days. You can mitigate the vulnerability by following the mitigations listed below.

Mitigations

Polycom recommends following standard best practices for Unified Communications, as detailed in our best practices paper found at:

http://support.polycom.com/global/documents/support/documentation/polycom_uc_security_best_pr actices_2015.pdf

As detailed in our best practices paper, Polycom specifically recommends that endpoints such as HDX be placed behind a firewall and not be directly accessible from the Internet.

In addition, Polycom recommends enabling HDX's "Secure Mode" by logging into the web UI > Admin Settings > Security > Security Settings and checking the box for "Secure Mode". This will require users to authenticate before they can access the HDX's diagnostics port.

Once the admin checks the box for Secure Mode they are prompted to enter a "room password" for the HDX. Polycom recommends making the password at least 12 characters long, using upper and lower case and special characters, and not containing easily-guessable strings like "polycom" or "password".

Recognition

Polycom appreciates and values the members of the security research community who find vulnerabilities, bring them to our attention, and work with Polycom in a coordinated effort so
that security fixes can be issued to all impacted customers. We would like to thank the independent security researchers at SensePost for discovering this vulnerability and alerting us.

CVSS v3 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 v3 Score:
8.0 - CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

For more information on CVSS v3 please see: https://www.first.org/cvss

Severity: Critical

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment or has questions about the solution or mitigation recommendations described above should contact Polycom Technical Support by calling 1-800-POLYCOM or visiting:

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

You might also find value in the latest high-level security guidance and security news from Polycom, which is located at:

http://www.polycom.com/security

Revision History

Revision 1.0 - Original publication: November 15, 2017
Revision 1.1 – Updated publication with Hotfix availability: November 15, 2017

以下、弊社にて日本語に翻訳

セキュリティ勧告：Polycom HDX に対する遠隔地からのコード実行の脆弱性

発行日: 2017 年 11 月 15 日

当勧告に記載される情報は変更される可能性があります

※こちらのドキュメントの最新バージョンは以下の URL に掲載されます

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

脆弱性概要：

HDX の診断ポート(port tcp/23)の Polycom shell(psh)機能に対し、重大な脆弱性が見つかりました。本脆弱性により、リモートの攻撃者が HDX 上で任意のコードを実行する可能性があり、これによりシステムが不正アクセスされる可能性があります。

影響のある製品：

HDX 3.1.11 hotfix 1 及びそれ以前	HDX 3.1.11 hotfix 2 またはそれ以降で修正済み

解決策：

以下の Polycom Support web site から利用できる、HDX 3.1.11 hotfix 2 以降へアップデートしてください。

http://support.polycom.com/content/support/North_America/USA/en/support/video/hdx_series.html

今後正規版(GA)のソフトウェアのリリースが予定されています。以下の緩和策を実施することで脆弱性の緩和が可能です。

緩和策：

Polycom はユニファイド・コミュニケーションに対し以下リンク先の最善策を推奨いたします。

http://support.polycom.com/global/documents/support/documentation/polycom_uc_security_best_practices_2015.pdf

最善策に記載の通り、HDX 等のエンドポイントは、ファイアーウォールより後方に配置し、インターネットから直接アクセスできないようにします。

加えて、Web ユーザーインターフェース＞管理者設定＞セキュリティ＞セキュリティ設定＞「セキュリティモード」にチェックを入れてセキュリティモードを有効にすることを推奨します。これは HDX の診断ポートにアクセスする前に、ユーザーに対し認証情報を要求します。

管理者がセキュアモードにチェックを入れることで、ルームパスワードの入力を促すことができます。パスワードは 12 文字以上、小文字、大文字、特殊文字を含めることを推奨します。また、簡単に推測される「polycom」または「password」のような文字は含めないでください。

御礼:

本脆弱性を発見し注意喚起を Polycom へ行い、そして影響を受けたお客様へのセキュリティフィックス発行のために尽力して頂いたセキュリティリサーチコミュニティに感謝します。本脆弱性の発見及び注意喚起を行っていただいた SensePost のセキュリティ研究員の皆様に重ねて御礼申し上げます。

共通脆弱性評価システム CVSS v3:

お客様の脆弱性の評価を支援するために、Polycom は共通脆弱性評価システム(CVSS)を使用します。このシステムはお客様へ情報システムの特性と影響を伝達するためにオープンフレームワークを提供し、お客様が情報に基づいた意思決定を行い、お客様の環境への影響を評価できるようにします。

Base CVSS v3 Score:

8.0 - CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

詳細については CVSS v3 をご確認ください: https://www.first.org/cvss

セキュリティレベル:重大

コンタクト：

本脆弱性を懸念されており影響を受けている端末を使用されているお客様へ、上記に推奨されている解決策または緩和策に対し質問があれば、Polycom Technical Support へ 1-800-POLYCOM によるお問合せまたはサイトの訪問をお願いします。

http://support.polycom.com/PolycomService/support/us/support/documentation/security_center.html

Polycom の最新の高セキュリティガイドまたはセキュリティに関するニュースは以下から確認可能です。

http://www.polycom.com/security

改定履歴：

改定 1.0 - 初版発行: 2017 年 11 月 15 日
改定 1.1 - 改訂版と利用可能な Hotfix: 2017 年 11 月 15 日

以上