2018 年 11 月 13 日

お客様各位

株式会社プリンストン

## セキュリティ勧告：RealPresence Group で発生したリモートで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。

2018 年 11 月 1 日にポリコム社から RealPresence Group シリーズ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」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 BULLETIN – Remote Code Execution Vulnerability Found in Group Series – Bulletin Version 1.0

# Security Bulletin Related to Remote Code Execution Vulnerability Found in Group Series

DATE PUBLISHED: November 1st , 2018

**Any information in this Bulletin is subject to change.**

Please Note: This is a living document and may be subject to updates. The newest version of this document can be found at the following URL:
https://support.polycom.com/content/support/security-center.html

### Vulnerability Summary

A new remote code execution vulnerability has been identified in Group Series. The vulnerability allows a remote attacker to execute arbitrary code which leads to the compromise of the system.

### Products Affected

Group Series running software versions 6.1.3, 6.1.4, 6.1.5 and 6.1.6 are affected by this vulnerability.

### Solution

Update Group Series to run software version 6.1.7 or later from the following URL:
https://support.polycom.com/PolycomService/home/home.htm

### 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 researcher Frank Cozijnsen from KPN for discovering this vulnerability, alerting us, and for cooperative disclosure.

## CVSS v3 Base Metrics:

To assist our customers in the evaluation of this vulnerability; Polycom uses 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 Scores:

CVE-2018-15128 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

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

## Severity: Critical

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.

以下、弊社にて日本語に翻訳

セキュリティに関する脆弱性 - RealPresence Groupで発生したリモートでのコード実行の脆弱性-Bulletin Version 1.0

リモートでコードが実行される脆弱性に関するセキュリティ情報
公開日:2018年11月1日

この掲示の情報は変更されることがあります。
注意:これは今現在の文書であり、更新の対象となる可能性があります。最新の文書は以下のURLにあります:
https://support.polycom.com/content/support/security-center.html

**脆弱性の概要**
新しいリモートコード実行の脆弱性がRealPresence Groupシリーズで確認されました。この脆弱性により、リモートの攻撃者は任意のコードを実行し、システムを損害させる恐れがあります。

**影響を受ける製品**
ソフトウェアバージョン6.1.3、6.1.4、6.1.5、および6.1.6のRealPresence Groupは、この脆弱性の影響を受けます。

**解決策**
以下のURLから、RealPresence Groupシリーズをソフトウェアバージョン6.1.7以上にアップデートします。
https://support.polycom.com/PolycomService/home/home.htm

**御礼**
ポリコムは、脆弱性を発見したセキュリティ研究コミュニティの方々に感謝いたします。その方々のおかげで影響を受けるすべてのお客様に対してにセキュリティ修正をお知らせすることができます。改めて、この脆弱性を発見したKPNの独立系セキュリティ研究者Frank Cozijnsen氏に感謝致します。

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。
ベースCVSS v3スコア:
CVE-2018-15128 9.8(CVSS:3.0 / AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:H)
CVSS v3の詳細については、https://www.first.org/cvssを参照してください。

**重要度**:クリティカル

**評価定義**
クリティカルな脆弱性が悪用された場合、悪質なコードが実行される可能性があります。
高度の脆弱性が悪用された場合、データの機密性、完全性、可用性、またはリソースの完全性または可用性に影響を与える可能性があります。
中程度の脆弱性は、デフォルト設定、監査などの要因によって著しく制限されているか、悪用されにくいものです。低度の脆弱性はシステムへの影響は最小限であり、悪用することは極めて困難です。

以上