複数のCisco TelePresence製品におけるコマンドインジェクションの脆弱性

Critical

アドバイザリーID : cisco-sa-20150513-tp　CVE-2015-0713
初公開日 : 2015-05-13 16:00
バージョン 1.0 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID : CSCur15855 CSCur15803 CSCur15825 CSCur15842 CSCur15832 CSCur15850 CSCur08993 CSCul55968 CSCur15807

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

複数のCisco TelePresence製品のWebフレームワークにおける脆弱性により、認証されたリモートの攻撃者が、 rootユーザの権限で実行される任意のコマンドを注入する可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、デバイスに認証され、巧妙に細工された入力を Web ページの該当パラメータに送信することで、この脆弱性をエクスプロイトする可能性があります。影響を受けるパラメータにアクセスするには、管理者権限が必要です。エクスプロイトに成功すると、攻撃者は rootユーザの権限でシステムコマンドを実行できる可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。これらの脆弱性に対しては回避策がありません。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150513-tp

該当製品

脆弱性のある製品

次の製品は、脆弱性のあるソフトウェアバージョンを実行している場合に影響を受けます。

- Cisco TelePresence Advanced Media Gateway Series
- Cisco TelePresence IP Gateway Series

- Cisco TelePresence IP VCR Series
- Cisco TelePresence ISDNゲートウェイ
- Cisco TelePresence MCU 4200 シリーズ
- Cisco TelePresence MCU 4500 シリーズ
- Cisco TelePresence MCU 5300 シリーズ
- Cisco TelePresence MCU MSE 8420
- Cisco TelePresence MCU MSE 8510
- Cisco TelePresence Serial Gateway Series
- Cisco TelePresence Server 7010
- Cisco TelePresence Server MSE 8710
- Cisco TelePresence Server on Multiparty Media 310
- Cisco TelePresence Server on Multiparty Media 320
- Cisco TelePresence Server on Virtual Machine

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

複数のCisco TelePresence製品のWebフレームワークにおける脆弱性により、認証されたリモートの攻撃者が、 rootユーザの権限で実行される任意のコマンドを注入する可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、デバイスに認証され、巧妙に細工された入力を Web ページの該当パラメータに送信することで、この脆弱性をエクスプロイトする可能性があります。影響を受けるパラメータにアクセスするには、管理者権限が必要です。エクスプロイトに成功すると、攻撃者は rootユーザの権限でシステムコマンドを実行できる可能性があります。

次の表に、影響を受ける各製品のこの脆弱性を特定するために使用するCisco Bug IDを示します。

製品名	Cisco Bug ID
Cisco TelePresence Advanced Media Gatewayシリーズソフトウェア	CSCur15855(登録ユーザ専用)
Cisco TelePresence IP Gatewayシリーズソフトウェア	CSCur15842(登録ユーザ専用)
Cisco TelePresence IP VCRシリーズソフトウェア	CSCul55968(登録ユーザ専用)
Cisco TelePresence ISDN Gatewayソフトウェア	CSCur15832(登録ユーザ専用)
Cisco TelePresence MCUソフトウェア	CSCur15825(登録ユーザ専用)

Cisco TelePresence MCU MSEソフトウェア	CSCur15807(登録ユーザ専用)
Cisco TelePresence Serial Gatewayシリーズソフトウェア	CSCur15850(登録ユーザ専用)
Cisco TelePresence Serverソフトウェア（ハードウェアおよび仮想マシン用）	CSCur15803(登録ユーザ専用)および CSCur08993(登録ユーザ専用)

この脆弱性に対してCommon Vulnerabilities and Exposures(CVE)IDとしてCVE-2015-0713が割り当てられています。

回避策

この脆弱性に対する回避策はありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories, Responses, and Alerts アーカイブや、後続のアドバイザリを参照して侵害の可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

次の表に、影響を受ける製品それぞれについて、この脆弱性を修正するリリースを示します。

製品名	修正済みリリース
Cisco TelePresence Advanced Media Gatewayシリーズソフトウェア	1.1 (1.40) 以降
Cisco TelePresence IP Gatewayシリーズソフトウェア	修正の予定はありません。製品はメンテナンスサポート終了です
Cisco TelePresence IP VCRシリーズソフトウェア	3.0 (1.27) 以降
Cisco TelePresence ISDN Gatewayソフトウェア	2.2 (1.94) 以降
Cisco TelePresence MCUソフトウェア	4.4 (3.54) 以降 4.5 (1.45) 以降
Cisco TelePresence MSE Supervisorソフトウェア	2.3 (1.38) 以降
Cisco TelePresence Serial Gatewayシリーズソフトウェア	1.0 (1.42) 以降
Cisco TelePresence Serverソフトウェア（ハードウ	ハードウェアリリースの3.1(1.98)

エアおよび仮想マシン用)	仮想マシンの4.1(1.79)

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

この脆弱性は、製品のセキュリティレビュー中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150513-tp

改訂履歴

リビジョン 1.0	2015年5月13日	初回公開リリース

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。