Cisco TelePresence ISDN Gateway Dチャネル のDoS脆弱性

High

アドバイザリーID : cisco-sa-20140122-isdngw
初公開日 : 2014-01-22 16:00
バージョン 1.0 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCui50360

CVE-2014-0660

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

Cisco TelePresence ISDN Gateway(ISDN GW)には、認証されていないリモートの攻撃者がデータチャネル（Dチャネル）のドロップをトリガーし、すべてのコールを終了させ、ユーザが新しいコールを発信するのを妨げる可能性のある脆弱性が存在します。

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。この脆弱性を軽減する回避策はありません。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-20140122-isdngw

該当製品

脆弱性のある製品

Cisco TelePresence ISDN GW 3241またはCisco TelePresence ISDN GW MSE 8321で稼働しているCisco TelePresence ISDN Gatewayソフトウェアの2.2(1.92)より前のすべてのリリースが、この脆弱性の影響を受けます。

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

Cisco TelePresence ISDN Gatewayは、Cisco TelePresence IPベースのビデオインフラストラクチャ製品およびIPベースのエンドポイントのISDNネットワーク接続を可能にする高性能ビデオゲ

ートウェイです。

Cisco TelePresence ISDN GatewayのISDN Q.931シグナリングプロトコルを処理するコードの脆弱性により、認証されていないリモートの攻撃者がデータチャネル（Dチャネル）のドロップを引き起こし、すべてのコールが終了し、ユーザが新しいコールを発信できなくなる可能性があります。

この脆弱性は、巧妙に細工されたQ.931 STATUSメッセージの不適切な処理に起因します。攻撃者は、巧妙に細工されたパケットをQ.931フローに挿入することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はDチャネルのドロップをトリガーできる可能性があります。その結果、影響を受けるシステムで処理されたすべてのアクティブコールが終了し、Dチャネル通信が回復するまで新しいコールを確立できなくなります。通常の動作に戻すには、ソフトウェアのリロードが必要です。

この脆弱性は、Cisco Bug ID CSCui50360(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2014-0660が割り当てられています。

回避策

この脆弱性を軽減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 のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、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。

この脆弱性は、Cisco TelePresence ISDN Gatewayソフトウェア2.2(1.92)以降で修正されています。

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、カスタマーサービスリクエストの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140122-isdngw

改訂履歴

リビジョン 1.0	2014年1月22日	初版リリース

利用規約

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。