Cisco Small Business シリーズ スイッチにおけるメモリ破損の脆弱性

High

アドバイザリーID : cisco-sa-20190703-sbss-memcorrupt

初公開日 : 2019-07-03 16:00

バージョン 1.0 : Final

CVSSスコア : 7.5

回避策 : No workarounds available

Cisco バグ ID : CSCvp43390

CVE-2019-1892

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 Small Business 200、300、および 500 シリーズ マネージド スイッチのセキュア ソケット レイヤ（SSL）入力パケット プロセッサの脆弱性により、認証されていないリモート攻撃者が該当デバイスでメモリの破損を引き起こす危険性があります。

この脆弱性は、HTTPS パケットの不適切な検証に起因します。 攻撃者は、該当デバイスの Web インターフェイスに不正な形式の HTTPS パケットを送信することにより、この脆弱性をエクスプロイトする可能性があります。 攻撃者は、エクスプロイトに成功すると、デバイスの予期しないリロードを発生させ、サービス妨害（DoS）状態を引き起こせるようになります。

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ました。 この脆弱性に対処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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sbss-memcorrupt

該当製品

脆弱性のある製品

この脆弱性は、HTTPS を許可するように管理 Web インターフェイスが設定されている、1.4.10.6 より前のソフトウェア リリースを実行している Cisco Small Business 200、300、お

よび 500 シリーズ マネージド スイッチに影響します。 このコマンドはデフォルトで有効になっています。

Web インターフェイスが HTTPS 用に設定されているかどうかを判断するために、管理者はデバイスの Web インターフェイスにログインし、[セキュリティ（Security）] > [TCP/UDPサービス（TCP/UDP Service）] に移動できます。 [HTTPSサービス（HTTPS Service）] フィールドの値は、機能が有効/無効になっているかどうかを示します。

脆弱性のある製品モデルの完全なリストについては、次のシスコ製品のリリースノートを参照してください。
200、300、および 500 シリーズ スイッチのリリース ノート。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Small Business 250、350、550 シリーズ スイッチ
- Small Business 220 シリーズ スマート スイッチ
- ESW2 シリーズ マネージド スイッチ

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性は、ソフトウェア リリース 1.4.10.6 以降で修正されています。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sbss-memcorrupt

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 7 月 3 日

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。