Cisco Firepower Threat Defense ソフトウェア署名の検証バイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-sigbypass-FcvPPCeP **初公開日 :** 2020-05-06 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.9 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvg16015	CVE-2020-3308

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 Firepower Threat Defense （ FTD ）ソフトウェアのイメージ署名の検証機能の脆弱性は影響を受けたデバイスで悪意のあるソフトウェアパッチをインストールする認証される、管理者レベル 資格情報が付いているリモート攻撃者可能にする可能性があります。

脆弱性はパッチ イメージのためのデジタル署名の不適当な確認が原因です。 攻撃者は無署名のソフトウェアパッチを細工 し、影響を受けたデバイスでロードすることによってこの脆弱性をシグニチャ チェックをバイパスするために不正利用する可能性があります。 正常な工クスプロイトは攻撃者が悪意のあるソフトウェアパッチ イメージを起動することを可能にする可能性があります。

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ソフトウェア アップデートを提供しています。 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-sigbypass-FcvPPCeP

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は Cisco FTD ソフトウェア リリースにリリース 6.2.2.1 より先に該当しました。

Ciscoソフトウェアリリースがパブリケーションの時に脆弱だった情報に関しては、このアドバイザリの修正済みソフトウェア セクションを参照して下さい。 最も完全な、現在の情報についてはこのアドバイザリの上でバグID の詳細 セクションを参照して下さい。

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のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

Cisco はこの脆弱性が Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアまたは Cisco Firepower Management Center （FMC）ソフトウェアに影響を与えないことを判別しました。

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

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。

修正済みリリース

Cisco FTD ソフトウェア

パブリケーションの時に、次の表のリリース情報は正確でした。 最も完全な、現在の情報についてはこのアドバイザリの上でバグID の詳細 セクションを参照して下さい。

左の列は Ciscoソフトウェアリリースをリストし、リリースがこの アドバイザリに記載される 脆弱性から影響を受けしたこの脆弱性のための修正が含まれていたかどうかリリースし、右の列は示します。

Cisco FTD メジャー リリース	この脆弱性に対する最初の修正リリース
先により 6.1.0[1]	修正済みリリースに移行します。
6.1.0	修正済みリリースに移行します。
6.2.0	修正済みリリースに移行します。

6.2.1	修正済みリリースに移行します。
6.2.2	6.2.2.1
6.2.3	脆弱性なし
6.3.0	脆弱性なし
6.4.0	脆弱性なし
6.5.0	脆弱性なし
6.6.0	脆弱性なし

1. Cisco FMC および FTD ソフトウェア リリース 6.0.1 以前については、メンテナンスが終了しています。 この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

Cisco FTD ソフトウェアの修正済みリリースにアップグレードするには、次のいずれかの操作を行います。

- Cisco Firepower Management Center（FMC）を使用して管理しているデバイスについては、FMC インターフェイスを使用してアップグレードをインストールします。 インストールが完了したら、アクセス コントロール ポリシーを再適用します。
- Cisco Firepower Device Manager（FDM）を使用して管理しているデバイスについては、FDM インターフェイスを使用してアップグレードをインストールします。 インストールが完了したら、アクセス コントロール ポリシーを再適用します。

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-sigbypass-FcvPPCeP

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	2020-MAY-06

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。