Cisco Unified Computing System Manager および Cisco Firepower 9000 のリモート コマンド実行の脆弱性

アドバイザリーID : cisco-sa-20160120-ucsm
初公開日 : 2016-01-20 16:00
最終更新日 : 2017-11-27 21:40
バージョン 1.5 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCur90888 CSCux10615

CVE-2015-6435

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 Unified Computing System (UCS) Manager および Cisco Firepower 9000 シリーズ アプライアンスの CGI スクリプトの脆弱性により、認証されていないリモートの攻撃者が Cisco UCS Manager または Cisco Firepower 9000 シリーズ アプライアンスで任意のコマンドを実行できる可能性があります。

この脆弱性は、CGI スクリプトのシェル コマンドの保護されていない呼び出しに起因します。攻撃者は、巧妙に細工された HTTP 要求を Cisco UCS Manager または Cisco Firepower 9000 シリーズ アプライアンスに送信することで、この脆弱性を不正利用することが可能です。この不正利用により、攻撃者は Cisco UCS Manager または Cisco Firepower 9000 シリーズ アプライアンスで任意の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-20160120-ucsm

該当製品

脆弱性のある製品

この脆弱性は、Cisco UCS Manager のバージョン 2.2.0 で導入されました。脆弱性が修正された最初のリリース (このアドバイザリの「修正済みソフトウェア」セクションに記載) より前のバージョン 2.2.x が影響を受けます。バージョン 2.1.x 以前のリリースはこの脆弱性の影響を受けません。

Firepower 9000 シリーズ向け FX-OS のバージョン 1.1.2 より前のリリースは影響を受けます。

管理者は、管理 GUI にログインすることで Cisco UCS Manager ソフトウェアのバージョンを確認できます。UCS Manager のバージョン番号は、 情報アイコンをクリックして表示されるポップアップ画面のバージョン フィールドに表示されます。

管理者は管理 GUI にログインすることで、Cisco Firepower 9000 シリーズ シャーシで実行している FX-OS ソフトウェアのバージョンを確認できます。FX-OS のバージョン番号は、 概要ページ上部のバージョン フィールドに表示されます。

脆弱性を含んでいないことが確認された製品

Cisco Integrated Management Controller はこの脆弱性の影響を受けないことが確認されています。

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。

回避策

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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。

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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。
http://www.cisco.com/c/ja_jp/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。

修正済みバージョン

Cisco UCS Manager
脆弱性が修正された最初の Cisco UCS Manager のリリースは、2.2(4b)、2.2(5a)、2.2(6a)、3.0(2e)、3.1(e)、およびそれ以降です。上記より前の 2.2.x バージョンはこの脆弱性の影響を受けます。ソフトウェアは Cisco Software Central からダウンロードできます。

Cisco Firepower 9000 シリーズ アプライアンス
脆弱性が修正された最初の Cisco Firepower 9000 シリーズ アプライアンスは 1.1.2 です。ソフトウェアは Cisco Software Central からダウンロードできます。

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。

出典

この脆弱性は、Jens Krabbenhoeft 氏によってシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160120-ucsm

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.5	アドバイザリのメタデータを更新。	—	Final	2017 年 11 月 27 日
1.4	修正された最初の Cisco UCSM バージョンを更新。	修正済みソフトウェア	Final	2016 年 2 月 25 日
1.3	修正された最初の Cisco UCSM バージョンを更新。	修正済みソフトウェア	Final	2016 年 1 月 27 日
1.2	2.2.x より前の Cisco UCS Manager バージョンが影響を受けることを明記しました。	脆弱性が存在する製品	Final	2016 年 1 月 22 日
1.1	スペルの間違いを修正。	出典	Final	2016 年 1 月 21 日
1.0	初回公開リリース	—	Final	2016 年 1 月 20 日

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。