Cisco Integrated Management Controller の特権昇格の脆弱性

High

アドバイザリーID : cisco-sa-20170419-cimc

初公開日 : 2017-04-19 16:00

最終更新日 : 2018-01-23 14:48

バージョン 1.4 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCve48825 CSCvd14591

CVE-2017-6619

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 Integrated Management Controller（IMC）の Web ベース GUI における脆弱性により、認証されたリモートの攻撃者が、該当のデバイスでユーザ権限を昇格させ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、巧妙に細工された HTTP 要求を該当デバイスに送信することにより、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、認証された攻撃者は、デバイスに設定されているユーザ アカウントの権限を昇格させることができる可能性があります。

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-20170419-cimc

該当製品

脆弱性のある製品

この脆弱性は、次の Cisco IMC ソフトウェア リリースに影響を与えます。

- 1.4(1) ~ 1.4(8)
- 1.5(1) ~ 1.5(9)
- 2.0(1) ~ 2.0(13)

- 3.0(1c)

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。

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。
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。
http://www.cisco.com/en/US/support/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、Cisco CIMC ソフトウェア バージョン 3.0.1d および 3.0.3a 以降で修正されています。 Cisco CIMC ソフトウェアは、ソフトウェア ダウンロード サイトで、[製品（Products）] > [サーバ（Servers）] > [ユニファイド コンピューティング（Unified Computing）] の順に選択してダウンロードできます（http://www.cisco.com/cisco/software/navigator.html）。

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

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc

改訂履歴

Version	Description	Section	Status	日付
1.4	製品のメタデータを更新。		Final	2018 年 1 月 23 日
1.3	バグ ID に CSCve48825 を追加。	ヘッダー（Cisco Bug ID）	Final	2017 年 10 月 3 日
1.2	該当製品セクションを変更。	該当製品	Final	2017 年 5 月 31 日
1.1	影響を受ける製品を更新。	該当製品	Final	2017 年 5 月 11 日
1.0	初回公開リリース		Final	2017 年 4 月 19 日

利用規約