Cisco Integrated Management Controller におけるリモート コード実行の脆弱性

アドバイザリーID : cisco-sa-20170419-cimc3
初公開日 : 2017-04-19 16:00
最終更新日 : 2018-01-23 13:45
バージョン 1.5 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCvg31284 CSCvd14578 CSCve48833

CVE-2017-6616

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、認証されていないリモート攻撃者が、該当のデバイスで不正なリモート コマンドを実行する可能性があります。

この脆弱性は、該当のソフトウェアが、ユーザからの HTTP 要求の一部として受信した特定の値を完全にサニタイズしていないことに起因します。攻撃者は、該当ソフトウェアに巧妙に細工された HTTP 要求を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。不正利用されると、認証されていない攻撃者が ルート レベルの権限でシステム コマンドを実行す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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc3

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際には、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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/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）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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc3

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	製品のメタデータを更新。	—	Final	2018 年 1 月 23 日
1.4	バグ ID に CSCvg31284 を追加。	ヘッダー（Cisco Bug ID）	Final	2017 年 10 月 25 日
1.3	バグ ID に CSCve48833 を追加。	ヘッダー（Cisco Bug ID）	Final	2017 年 10 月 3 日
1.2	脆弱性の存在するリリースを追加。	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

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。

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。