Cisco Integrated Management Controller の CSR 生成コマンド インジェクションにおける脆弱性

High

アドバイザリーID : cisco-sa-20190821-imc-cmdinject-1896

初公開日 : 2019-08-21 16:00

最終更新日 : 2020-08-26 14:48

バージョン 1.1 : Final

CVSSスコア : 7.2

回避策 : No workarounds available

Cisco バグ ID : CSCvo36057

CVE-2019-1896

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 ベースの管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、任意のコマンドを注入してルート権限を取得する可能性があります。

この脆弱性は、Web ベースの管理インターフェイスの証明書署名要求（CSR）機能において、ユーザが行った入力の検証が不十分であることに起因します。攻撃者は、Web ベースの管理インターフェイスに巧妙に細工された CSR を送信して、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、管理者権限を持つ攻撃者は完全なルート権限を使用してデバイス上で任意のコマンドを実行することができます。

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-20190821-imc-cmdinject-1896

該当製品

脆弱性のある製品

この脆弱性は、Cisco IMC ソフトウェアの脆弱性のあるリリースを実行している次のシスコ製

品に影響を与えます。

- スタンドアロン モードになっている UCS C シリーズおよび S シリーズ サーバ
- UCS E シリーズ サーバ
- 5000 シリーズ エンタープライズ ネットワーク コンピューティング システム（ENCS）プラットフォーム

該当するソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

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。

シスコは、この脆弱性が UCS Manager によって管理される以下の Cisco FI 接続サーバには影響を与えないことを確認しました。

- UCS B シリーズ サーバ
- UCS C シリーズ サーバ
- UCS S シリーズ サーバ

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

シスコでは、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、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。
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、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを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

Cisco UCS C シリーズおよび S シリーズ サーバ

次の表に示すように、適切な Cisco UCS C シリーズおよび S シリーズ ソフトウェア リリースにアップグレードすることをお勧めします。

Cisco IMC ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
1.4	脆弱性なし
1.5	脆弱性なし
2.0	2.0(13o)
3.0	3.0(4k)
4.0	4.0(2f)、4.0(4b)

Cisco IMC ソフトウェアは、Cisco.com の Software Center にアクセスし、次の手順でダウンロードできます。

1. [すべて参照（Browse all）] をクリックします。
2. [サーバ: ユニファイドコンピューティング（Servers - Unified Computing）] > [UCS Cシリーズラックマウントスタンドアロンサーバソフトウェア（UCS C-Series Rack-Mount Standalone Server Software）] にアクセスします。
3. 右側のペインで、適切な Cisco UCS C シリーズ プラットフォームを選択します。
4. [ソフトウェアの種類の選択（Select a Software Type）] **ページで、[ユニファイドコンピューティングシステム(UCS)サーバファームウェア（Unified Computing System (UCS) Server Firmware）]** をクリックします。
5. ページの左側のペインを使用してリリースにアクセスします。

Cisco UCS E シリーズ サーバ

シスコは、Cisco UCS E シリーズ サーバ向けの Cisco IMC ソフトウェア リリース 3.2(8) でこの脆弱性を修正しました。

このソフトウェアは Cisco.com の Software Center にアクセスし、次の手順でダウンロードできます。

1. [すべて参照（Browse all）] をクリックします。
2. [サーバ: ユニファイドコンピューティング（Servers - Unified Computing）] > [UCS Eシリーズソフトウェア（UCS E-Series Software）] にアクセスします。
3. 右側のペインで、適切な Cisco UCS E シリーズ プラットフォームを選択します。
4. [ソフトウェアの種類の選択（Select a Software Type）] **ページで、[ユニファイドコンピューティングシステム(UCS)サーバファームウェア（Unified Computing System (UCS) Server Firmware）]** をクリックします。
5. ページの左側のペインを使用してリリースにアクセスします。

Cisco 5000 シリーズ エンタープライズ ネットワーク コンピューティング システム プラットフォーム

シスコは、Cisco 5000 シリーズ ENCS プラットフォーム向けの Cisco IMC ソフトウェア リリース 3.2(8) でこの脆弱性を修正しました。

このソフトウェアは Cisco.com の Software Center にアクセスし、次の手順でダウンロードできます。

1. [すべて参照（Browse all）] をクリックします。
2. [ルータ（Routers）] > [ネットワーク機能の仮想化（Network Functions Virtualization）] > [5000シリーズエンタープライズネットワークコンピューティングシステム（5000 Series Enterprise Network Compute System）] にアクセスします。
3. 右側のペインで、適切な ENCS プラットフォームを選択します。
4. [ソフトウェアの種類の選択（Select a Software Type）] **ページで、[ENCSソフトウェア（ENCS Software）]** をクリックします。
5. ページの左側のペインを使用してリリースにアクセスします。

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

この脆弱性は、シスコ内部でセキュリティテストを実施中、シスコの M.S によって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1896

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	この脆弱性の報告者を公表するために更新。	出典	最終版	2019 年 8 月 26 日
1.0	初回公開リリース	—	最終版	2019 年 8 月 21 日

利用規約