Cisco Identity Services Engine における特権昇格の脆弱性

High

アドバイザリーID : cisco-sa-20171101-ise

初公開日 : 2017-11-01 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCve74916

CVE-2017-12261

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

SSH でアクセスできる Cisco Identity Services Engine（ISE）の制限付きシェルにおける脆弱性により、認証を受けているローカル攻撃者が、昇格された特権で任意の CLI コマンドを実行する可能性があります。

この脆弱性は、制限付きシェルで実行された CLI コマンドへのユーザ入力に対する検証が不完全なことに起因するものです。 この脆弱性は、ターゲット デバイスへの認証および特権昇格につながり得るコマンドの実行を攻撃者が行うことで不正利用される可能性があります。 攻撃者がこの脆弱性を不正利用するには、デバイスに対する有効なユーザ クレデンシャルが必要です。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-20171101-ise

該当製品

脆弱性のある製品

この脆弱性は、リリース 1.4、2.0、2.0.1、2.1.0 を実行している下記 Cisco Identity Services Engine（ISE）製品に影響します。

- Cisco ISE

- Cisco ISE Express
- Cisco ISE Virtual Appliance

デバイス上で実行しているソフトウェアのリリースを確認するには、管理者がデバイスの CLI で **show version コマンド**を使用するか、管理ポータルの右上隅で [Settings（設定、歯車アイコン）] > [**About Identity Service Engine (ソフトウェア情報)**] をクリックします。 CLI コマンドの出力は、次の例のようになります。

```
ServiceEngine115/admin# show version

ServiceEngine115/admin# show version

ServiceEngine115/admin# show version

ServiceEngine115/admin# show version
```

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。

脆弱性が Cisco ISE Passive Identity Connector に影響しないことはシスコで確認済みです。

詳細

セキュリティ侵害の痕跡

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

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco Identity Services Engine のリリース	この脆弱性に対する最初の修正リリース
1.3	影響あり。 1.4 パッチ 12 への移行が必要
1.4	1.4 パッチ 12（メモを参照して下さい）
2.0	2.0 パッチ 6（メモを参照して下さい）
2.0.1	該当： 2.1 パッチへの移行する 5
2.1.0	2.1 パッチ 5
2.2.0	2.2.0 パッチ 2
2.3.0	Not affected

注: ソフトウェア リリース 1.4 パッチ 12 および 2.0 パッチ 6 は、現時点では掲載されていません。 これらのリリースが掲載されるまでは、修正済みリリースへの移行によって対処してください。

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、匿名のセキュリティ研究者によってシスコに報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-ise

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 11 月 1 日

利用規約