Cisco Prime InfrastructureおよびCisco Evolved Programmable Network Managerのコマンドインジェクションの脆弱性

High

アドバイザリーID : cisco-sa-pi-epnm-cmd-inj-YU5e6tB3

CVE-2021-1487

初公開日 : 2021-05-19 16:00

バージョン 1.0 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvw07763 CSCvw67903

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 Prime InfrastructureおよびEvolved Programmable Network(EPN)ManagerのWebベース管理インターフェイスの脆弱性により、認証されたリモート攻撃者が該当システム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、Webベースの管理インターフェイスへのユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたHTTP要求をインターフェ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。エクスプロイトが成功すると、攻撃者は特定の非ルートユーザの権限を使用して、基盤となるオペレーティングシステム(OS)上で任意のコマンドを実行する可能性があります。これにより、攻撃者は影響を受けるシステムを制御し、機密データを取得して変更できるようになります。攻撃者は、任意の設定ファイルをプッシュし、デバイスのクレデンシャルと機密情報を取得し、最終的にデバイスの安定性を低下させ、サービス拒否(DoS)状態を引き起こすことで、該当システムによって管理されるデバイスにも影響を与えます。

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-pi-epnm-cmd-inj-YU5e6tB3

該当製品

脆弱性のある製品

この脆弱性は、リリース3.9より前のCisco Prime Infrastructureリリースおよびリリース5.1より前のCisco EPN Managerリリースに影響を与えます。

脆弱性が存在する Cisco 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」セクション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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

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。
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、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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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 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。
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

この脆弱性は、次のリリースで修正されています。

- Cisco Prime Infrastructureリリース3.9以降
- Cisco EPN Managerリリース5.1以降

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-cmd-inj-YU5e6tB3

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	最終版	2021年5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。