

Cisco Prime Infrastructure および Evolved Programmable Network Manager DOM クロスサイト スクリプティング脆弱性

Medium	アドバイザーID : cisco-sa-20170621-piepnm4	CVE-2017-6700
	初公開日 : 2017-06-21 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 4.7	
	回避策 : Yes	
	Cisco バグ ID : CSCvc49586 , CSCvc24620	

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 (PI) および Evolved Programmable Network Manager (EPNM) のウェブベースの管理インターフェイスの脆弱性はリモート攻撃者非認証が影響を受けたデバイスのウェブベースの管理インターフェイスのユーザに対してドキュメント オブジェクト モデル (DOM) 基づいた (環境がクライアント側) クロスサイト スクリプティング (XSS) 攻撃を行なうようにする可能性があります。

脆弱性は影響を受けたデバイスのウェブベースの管理インターフェイスによってユーザが指定する入力の不十分な検証が原因です。 攻撃者はインターフェイスのユーザの巧妙に細工されたリンクをクリックするように説得によってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が任意スクリプト コードをインターフェイスという点において実行するか、または攻撃者が敏感なブラウザ ベースの情報にアクセスするようにことを可能にする可能性があります。

DOM ベースの XSS 不正侵入および潜在的な軽減についてのその他の情報はで見つけることができます:

- https://www.owasp.org/index.php/DOM_Based_XSS
- https://www.owasp.org/index.php/Types_of_Cross-Site_Scripting#DOM_Based_XSS_28AKA_Type#029

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-20170621-piepnm4>

影響を受ける製品

脆弱性が存在する製品

この脆弱性は Cisco Prime Infrastructure および Evolved Programmable Network Manager に影響を与えます。該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

脆弱性が存在しない製品

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。

細部

回避策

この脆弱性に対処する回避策はありません。

固定ソフトウェア

修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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。

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。

ソース

シスコは、識別された脆弱性を報告してくださった SEC Consult Vulnerability Lab の Pichaya Morimoto 氏 (発見、分析、対応) に感謝いたします。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170621-piepnm4>

改訂履歴

Version	Description	Section	Status	Date
1.0	Initial public release.		Final	2017-June-21

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、単独の転載や意識を施した場合、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。