Cisco Data Center Network Manager ソフトウェアの多重 脆弱点

Medium	**アドバイザリーID :** cisco-sa-20171129-dcnm **初公開日 :** 2017-11-29 16:00 **最終更新日 :** 2017-11-30 12:25 **バージョン 1.1 :** Final **CVSSスコア :** 6.1 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvf68235 CSCvf68247 CSCvf63150 CSCvf68218 CSCvf40477	CVE-2017-12346 CVE-2017-12347 CVE-2017-12344 CVE-2017-12345 CVE-2017-12343

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 Data Center Network Manager（DCNM）ソフトウェアの多重 脆弱点はリモート攻撃者が任意の値を DCNM コンフィギュレーションパラメータにインジェクトするか、ユーザを悪意のある Webサイトにリダイレクトするか、悪意のあるコンテンツを DCNM クライアントインターフェイスにインジェクトするか、または影響を受けたソフトウェアのユーザに対してクロスサイトスクリプティング（XSS）攻撃を行なうことを可能にする可能性があります。

これらの脆弱性に関する詳細については、この Security Advisory の" Details " セクションを参照して下さい。

これら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。
129-dcnm

該当製品

脆弱性のある製品

これらの脆弱性は最初の修正済みリリース前に Cisco Data Center Network Manager（DCNM）ソフトウェアのすべてのリリースに該当します。 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。

詳細

Cisco Data Center Network Manager（DCNM）ソフトウェアの 5 脆弱性はリモート攻撃者が任意の値を DCNM コンフィギュレーションパラメータにインジェクトするか、ユーザを悪意のあるWebサイトにリダイレクトするか、悪意のあるコンテンツを DCNM クライアントインターフェイスにインジェクトするか、または影響を受けたソフトウェアのユーザに対してクロスサイト スクリプティング（XSS）攻撃を行なうことを可能にする可能性があります。

脆弱性は互いに依存していません; 脆弱性の 1 の不正利用が別の脆弱性を不正利用するために必要となりません。 さらに、脆弱性の 1 から影響を受けするソフトウェア リリースは他の脆弱性から影響を受けしないかもしれません。

脆弱性についての詳細は次の通りです。

Cisco Data Center Network Manager バイパス クライアント側の検証パラメータ脆弱性

Cisco DCNM ソフトウェアのウェブベースの管理インターフェイスの脆弱性は影響を受けたシステムのための DCNM コンフィギュレーションパラメータに任意の値をインジェクトする認証される、リモート攻撃者可能にする可能性があります。

脆弱性は影響を受けたソフトウェアに送信 される HTTP ペイロードのユーザが指定するデータの不十分なサーバー側の検証が原因です。 攻撃者はサーバ側の保護をバイパスし、影響を受けたソフトウェアのためのある特定のコンフィギュレーションパラメータに任意の値をインジェクトすること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 DCNM コンフィギュレーションパラメータに任意の値をインジェクトすることを可能にする可能性があります。

この脆弱性のための CVE ID は次のとおりです: CVE-2017-12343

この脆弱性のためのセキュリティ へ の 影響 定格（ ）は次のとおりです: 中間

Cisco Data Center Network Manager HTTP ヘッダ インジェクト脆弱性

Cisco DCNM ソフトウェアの Webインターフェイスの脆弱性は攻撃者制御 Webサイト リダイレクトするように非認証が、リモート攻撃者に影響を受けたインターフェイスのユーザを悪意のあるする、可能性があります。

脆弱性は影響を受けたソフトウェアの Webインターフェイスに送られる HTTP ヘッダ パラメータの値の不十分な入力の検証が原因です。 攻撃者はユーザを悪意のあるリンクをクリックするように説得し、影響を受けたソフトウェアで送受信される HTTP メッセージに悪意のある HTTP ヘッダをインジェクトすること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悪意のある、攻撃者制御 Webサイトに影響を受けたソフトウェアのユーザをリダイレクトすることを可能にする可能性があります。

この脆弱性のための CVE ID は次のとおりです: CVE-2017-12344

この脆弱性のための次のとおりです: 中間

Cisco Data Center Network Manager コンテンツ スプーフィング脆弱性

Cisco DCNM ソフトウェアの Web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インターフェイスによって表示する コンテンツに悪意のあるコンテンツをインジェクトするようにする可能性があります。

脆弱性は影響を受けたソフトウェアの Webインターフェイスに送られる HTTP パラメータのユーザが指定する値の不十分な入力の検証が原因です。 攻撃者は影響を受けたソフトウェアに送られる HTTP メッセージに悪意のある HTTP パラメータ値をインジェクトすること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攻撃者がユーザを悪意のある手順に従うか、または悪意のあるリンクをクリックするように説得することを可能にする可能性がある、影響を受けたソフトウェアの Webインターフェイスによって表示する コンテンツに悪意のあるコンテンツをインジェクトすることを可能にする可能性があります。

この脆弱性のための CVE ID は次のとおりです: CVE-2017-12345

この脆弱性のための次のとおりです: 中間

Cisco Data Center Network Manager によって保存されるクロスサイト スクリプティング脆弱性

Cisco DCNM ソフトウェアのウェブベースの管理インターフェイスの脆弱性は非認証が、リモート攻撃者 攻撃者が任意スクリプト コードを実行するか、または敏感なブラウザ ベースの情報にアクセスすることを可能にする可能性がある影響を受けたインターフェイスのユーザに対して保存された 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ソフトウェア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。 攻撃者は影響を受けたインターフェイスのユーザの悪意のある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、または攻撃者がユーザのシステムの敏感なブラウザ 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。

この脆弱性のための CVE ID は次のとおりです: CVE-2017-12346

この脆弱性のための次のとおりです: 中間

Cisco Data Center Network Manager によって反映されるクロスサイト スクリプティング脆弱性

Cisco DCNM ソフトウェアのウェブベースの管理インターフェイスの脆弱性は非認証が、リモート攻撃者 攻撃者が任意スクリプト コードを実行するか、または敏感なブラウザ ベースの情報にアクセスすることを可能にする可能性がある影響を受けたインターフェイスのユーザに対して反映された 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ソフトウェア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。 攻撃者は影響を受けたインターフェイスのユーザの悪意のある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、または攻撃者がユーザのシステムの敏感なブラウザ 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。

この脆弱性のための CVE ID は次のとおりです: CVE-2017-12347

この脆弱性のための次のとおりです: 中間

回避策

これら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

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不正利用事例とその公表は確認しておりません。

出典

Cisco はこれらの脆弱性を報告するためにアプリケーションセキュリティ コンサルタント Indrajith.A.N に感謝することを望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-dcnm

改訂履歴

Version	Description	Section	Status	日付
1.1	CVE-2017-12343 のための脆弱性の詳細な説明を訂正して下さい。	Details	Final	2017-November-30
1.0	初回公開リリース		Final	2017-November-29

利用規約