

Cisco Prime Network Registrar の DHCP サーバで確認されたサービス妨害の脆弱性



アドバイザリーID : cisco-sa-cpnr-dhcp-dos-[CVE-2020-](#)

BkEZfhLP

[3272](#)

初公開日 : 2020-05-20 16:00

バージョン 1.0 : Final

CVSSスコア : [7.5](#)

回避策 : Yes

Cisco バグ ID : [CSCvs77733](#)

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 Network Registrar の DHCP サーバで脆弱性が確認されました。認証されていないリモートからの攻撃者が、該当デバイスでサービス妨害 (DoS) 状態を引き起こす可能性があります。

この脆弱性は、DHCP の受信トラフィックの入力検証が不十分であることに起因します。細工された DHCP 要求が該当デバイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、DHCP サーバプロセスの再起動を引き起こすことが可能になるため、DoS 状態に陥る恐れがあります。

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。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpnr-dhcp-dos-BkEZfhLP>

該当製品

脆弱性のある製品

この脆弱性は、Cisco Prime Network Registrar に影響を与えます。

脆弱性が存在する Cisco Prime Network Registrar リリースの詳細については、このアドバイザリーの「[修正済みソフトウェア](#)」の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

修正済みリリースにアップグレードできない場合には、回避策があります。回避策の実装の調整に関しては、[Cisco Technical Assistance Center \(TAC \)](#) にお問い合わせください。

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 <https://www.cisco.com/c/en/us/products/end-user-license-agreement.html> に記載の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。

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です。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、[シスコのセキュリティアドバイザリおよびアラート (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。

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 (https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) に連絡してアップグレードを入手してください。

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 Prime Network Registrar のメジャーリリース	最初の修正済みバージョン
8.3 より前	脆弱性なし
8.3	8.3.7.1
9.0	9.1.3
9.1	9.1.3
10.0	10.1.0.1
10.1	10.1.0.1

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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpnr-dhcp-dos-BkEZfhLP>

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	—	Final	2020 年 5 月 20 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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。