Cisco Video Surveillance 8000 シリーズ IP カメラの Cisco Discovery Protocol におけるリモートコード実行とサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-cdp-rcedos-mAHR8vNx

初公開日 : 2020-10-07 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 : CSCvv21695

CVE-2020-3544

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 Video Surveillance 8000シリーズIPカメラのCisco Discovery Protocol実装の脆弱性により、認証されていない隣接する攻撃者が該当デバイスで任意のコードを実行したり、デバイスをリロードしたりする可能性があります。

この脆弱性は、IPカメラがCisco Discovery Protocol(CDP)パケットを処理する際のチェックが欠落していることに起因します。この脆弱性は、該当デバイスに悪意のある Cisco Discovery Protocol パケットを送信することでエクスプロイトされる可能性があります。エクスプロイトに成功すると、攻撃者は該当 IP カメラでコードを実行したり、該当 IP カメラの予期せぬリロードを引き起したりすることが可能になり、結果としてサービス妨害（DoS）状態が発生する可能性があります。

注：Cisco Discovery Protocol はレイヤ 2 プロトコルです。この脆弱性をエクスプロイトするには、攻撃者は該当デバイスと同じブロードキャストドメイン内に存在する（レイヤ 2 と隣接関係にある）必要があります。

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ました。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-cdp-rcedos-mAHR8vNx

該当製品

脆弱性のある製品

この脆弱性は、リリース 1.0.9-5 より前のファームウェアリリースが実行され、Cisco Discovery Protocol が有効になっている Cisco Video Surveillance シリーズ IP カメラに影響を及ぼします。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Video Surveillance 3000 シリーズ IP カメラ
- Video Surveillance 4000 シリーズ高解像度 IP カメラ
- Video Surveillance 4300E 高解像度 IP カメラ
- Video Surveillance 4500E 高解像度 IP カメラ
- Video Surveillance 6000 シリーズ IP カメラ
- Video Surveillance 7000 シリーズ IP カメラ
- Video Surveillance PTZ IP Cameras

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

シスコでは、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、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、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを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。
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

シスコは、Cisco Video Surveillance 8000 シリーズ IP カメラのファームウェアリリース 1.0.9-5 以降でこの脆弱性を修正しました。

Cisco.com の Software Center からファームウェアをダウンロードするには、以下の手順を実行します。

1. [すべて参照（Browse all）] をクリックします。
2. [コネクテッドセイフティおよびセキュリティ（Connected Safety and Security）] > [Video Surveillance IPカメラ（Video Surveillance IP Cameras）] > [Video Surveillance 8000シリーズIPカメラ（Video Surveillance 8000 Series IP Cameras）] の順に選択します。
3. 適切な IP カメラのモデルを選択します。
4. [Video Surveillance 8000シリーズIPカメラファームウェア（Video Surveillance 8000 Series IP Camera Firmware）] をクリックします。
5. 製品ページの左ペインからリリースを選択します。

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

シスコは、この脆弱性について報告してくださった Qihoo 360 社 Nirvan Team の Qian Chen 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cdp-rcedos-mAHR8vNx

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース	—	最終版	2020 年 10 月 7 日

利用規約