機密性1（低）情報
（重要インフラ事業者等への配布可）

令和5年10月18日

Cisco IOS XEソフトウェアにおける ゼロデイ脆弱性(CVE-2023-20198) について

警察庁サイバー警察局
情報技術解析課
サイバーテロ対策技術室

1. 概要

- Cisco Systems社は10月16日(現地時間)に同社のネットワーク機器のオペレーティングシステム製品であるCisco IOS XE ソフトウェアにおけるゼロデイ脆弱性(CVE-2023-20198)についてのアドバイザリを公開した。[7.参考(1)]
- 本脆弱性を悪用することで、攻撃者は遠隔から認証を回避して機器上に特権を持つユーザアカウントを作成し、機器を制御することができる。
- 同社は本脆弱性を悪用した攻撃の発生を確認したとしている。

2. 脆弱性の CVSS スコア

- 脆弱性の深刻度の指標には共通脆弱性評価システムCVSS (Common Vulnerability Scoring System) というものがある。
- Cisco Systems社はこの脆弱性のCVSSによる深刻度を **10.0**としている。
- IPAによるCVSSの基本値の深刻度レベル分けでは

  緊急：9.0～10.0

  重要：7.0～8.9

  警告：4.0～6.9

  注意：0.1～3.9

  となっており、**10.0**は**緊急**レベルの深刻度である。

※ 脆弱性そのものの特性を評価したものが基本値、攻撃コードや対策情報の有無のような現在の深刻度を評価したものが現状値となっている。

3. 影響範囲

- Cisco Systems社が公開しているアドバイザリによると
  Cisco IOS XEソフトウェアを搭載したネットワーク機器に
  おいて「Web UI」機能が有効化されている場合に脆弱性の
  影響を受ける。[7.参考(1)]
- 機器の設定において下記のコマンド

  ip http server

  ip http secure-server

  のいずれか又は両方が含まれている場合は「Web UI」機能
  が有効化されている。（詳細は同社のアドバイザリ[7.参考
  (1)]を参照）

補足:
「Web UI」・・・機器に組み込まれたGUIベースのシステム管理ツール

4. 攻撃の発生状況

- Cisco Systems社は10月16日(現地時間)時点において、本脆弱性を悪用した攻撃の発生を確認したとしている。[7.参考(1)]
- サイバーセキュリティ関連のNPOであるShadowserver Foundationの観測によると、全世界で32,800以上のCisco IOS XEが動作しているIPアドレスが既に侵害されている(日本では361のIPアドレスが該当)。[7.参考(2)]

5. 対策

- Cisco Systems社は10月17日(日本時間)時点で、脆弱性の修正プログラムを提供しておらず、準備でき次第提供予定としている。[7.参考(1)]
- 脆弱性の修正プログラムが提供され次第、速やかに適用する。
- 同社はインターネットからアクセスできる本脆弱性の影響を受ける機器において、HTTPサーバ機能を無効化することを強く推奨している。(詳細は同社のアドバイザリ[7.参考(1)]を参照)

5. 対策

- [6. 攻撃の有無の確認]で機器が攻撃を受けた可能性があると判明した場合は、ネットワーク内の別のサーバ等が侵害されていないかを確認する。

6. 攻撃の有無の確認

- Cisco Systems社は、攻撃者が本脆弱性を悪用することで機器上にローカルユーザアカウントを作成し、不正プログラムをインストールした事例を確認したとしている。[7.参考(3)]
- 同社は攻撃の有無の確認方法として以下を提示している。(詳細は同社のアドバイザリ[7.参考(1)]を参照)

確認方法
機器のシステムログに、ユーザ名が「cisco_tac_admin」、「cisco_support」又はネットワーク管理者に心当たりのないローカルユーザとなっているメッセージが記録されていないか確認する。
機器のシステムログに、正常なインストール作業とは無関係な不審な名称のファイル名が記録されていないか確認する。

6. 攻撃の有無の確認

- Cisco Systems社は機器上に不正プログラムがインストールされているかを確認する方法として以下を提示している。(詳細は同社のアドバイザリ[7.参考(1)]を参照)

確認方法
機器に接続できる端末から以下のコマンド `curl -k -X POST "https://[機器のIP]/webui/logoutconfirm.html?logon_hash=1"` を実行して16進数の文字列の応答が返された場合は、不正プログラムがインストールされている。

6. 攻撃の有無の確認

- Cisco Systems社は攻撃を検知する方法として以下のSnort ruleを提示している。(詳細は同社のアドバイザリ[7.参考(1)]を参照)

ID	内容
3:50118:2	最初の不正プログラムのインストールに関する検知
3:62527:1	不正プログラムの通信内容に関する検知
3:62528:1	不正プログラムの通信内容に関する検知
3:62529:1	不正プログラムの通信内容に関する検知

6. 攻撃の有無の確認

- Cisco Systems社は攻撃に関連するIPアドレスの情報を公開しており、同社のアドバイザリに記載されている手順と合わせて、上述のIPアドレスに基づく攻撃の有無の確認を行う。([7.参考(3)])

7. 参考

(1) Cisco IOS XE Software Web UI Privilege Escalation Vulnerability
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

(2) Shadowserver FoundationのX(Twitter)の投稿
https://twitter.com/Shadowserver/status/1714483336876355873

7. 参考

(3) Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability
https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

(4)「Cisco IOS XE」にゼロデイ脆弱性 - 侵害有無の確認を
https://www.security-next.com/150233

(5)「Cisco IOS XE」のゼロデイ脆弱性、9月中旬ごろより悪用か
https://www.security-next.com/150237

7. 参考

(6) 米当局、「Cisco IOS XE」に判明したゼロデイ脆弱性について注意喚起
https://www.security-next.com/150244

(7) Cisco warns of new IOS XE zero-day actively exploited in attacks
https://www.bleepingcomputer.com/news/security/cisco-warns-of-new-ios-xe-zero-day-actively-exploited-in-attacks/

8. 変更履歴

- 10月18日　初版