Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer ungepatchten Schwachstelle in Cisco IOS XE

CSW-Nr. 2023-275141-1332, Version 1.3, 25.10.2023

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 16. Oktober veröffentlichte Cisco ein Advisory [CISCO23] zu einer ungepatchten und aktiv ausgenutzten Schwachstelle in der Web UI von IOS XE. Die Schwachstelle mit der Kennung CVE-2023-20198 ermöglicht es, entfernten, nicht-authentifizierten Angreifenden neue Accounts (mit Level 15 Zugriffsrechten) auf dem betroffenen System anzulegen. Angreifende sind somit in der Lage, Kontrolle über betroffene IOS XE Systeme zu erlangen und die Geräte zu kompromittieren, auf denen die Software eingesetzt wird (Swiches, Router, WLAN Controller). Die Schwachstelle hat die höchste CVSS-Bewertung von 10.0 ("kritisch") erhalten.

Betroffen sind physische und virtuelle Geräte mit IOS XE, deren Weboberfläche (Web UI) aktiviert ist. Eine besondere Gefährdung besteht, sollten diese aus dem Internet erreichbar sein.

Die Weboberfläche ist ein GUI-basiertes System-Management Tool zur Vereinfachung der Bereitstellung, Inbetriebnahme und des Managements von Cisco IOS XE Systemen. Sie wird standardmäßig mit ausgeliefert und muss nicht explizit aktiviert oder installiert werden. Die Oberfläche stellt eine benutzerfreundliche Alternative zur Administration dar, ohne Command Line Interfaces verwenden zu müssen. Die Oberfläche sollte jedoch nach Empfehlung von Cisco nicht aus dem Internet oder nicht-vertrauenswürdigen Netzwerken erreichbar sein [CISCO23].

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Ein Patch für die Schwachstelle **steht bislang nicht zur Verfügung**, Cisco verweist auf notwendige **Mitigationsmaßnahmen**. Ebenfalls hat Cisco eine **aktive Ausnutzung** der Schwachstelle beobachtet [CISCO23]. In einem Beitrag von Cisco Talos [TALOS23] wird berichtet, dass die ersten Angriffe auf die Schwachstelle bereits am 18. September stattfanden.

Update 1:
Nach Analysen von Censys [CENS23] wurden bereits mehr als 35.000 Cisco IOS XE Geräte kompromittiert.

Switches des Herstellers "Rockwell Automation" (Stratix® 5200, 5800) sind ebenfalls von der Schwachstelle durch den Einsatz von Cisco IOS XE auf diesen Geräten betroffen [ROCK23].

Update 2:
Bleepingcomputer [BLEE23] berichtete am 22. Oktober von einer stark eingebrochenen Anzahl an kompromittierten Geräten laut Scans. Die Gründe hierfür sind nicht bekannt, es ist möglich, dass die Angreifenden die Malware aktualisiert haben und die Erkennung nach den alten Merkmalen nicht mehr möglich ist. [BLEE23]

Am 22. Oktober hat Cisco erste Patches (17.9.4a) bereitgestellt, weitere Versionen werden ebenfalls zeitnah ein Update erhalten. Zu den behebenden Versionen zählen 17.9.4a, 17.6.6a, 17.3.8a und 16.12.10a. Der Stand der Veröffentlichung ist im Advisory [CISCO23] zu finden. Die Schwachstelle CVE-2023-20273 wurde im Advisory aufgenommen und wird ebenfalls in den Patches behoben. Diese Schwachstelle wurde von den Angreifenden ausgenutzt, um root Zugriff zu erlangen und die Malware auf das Dateisystem zu schreiben. [CISCO23]

Update 3:
Die stark eingeborchene Anzahl an gefundenen kompromittierten Geräten konnte auf eine Aktualisierung der Malware zurückgeführt werden [TALOS23]. Es stehen mittlerweile neue Erkennungstechniken bereit [GITH23].

Bewertung

Die weite Verbreitung von Cisco-Produkten wie Router, Switches und WLAN Controller (mit IOS XE) in relevanten Branchen sowie die bereits von Cisco beobachtete Ausnutzung, ergeben eine ernstzunehmende Gefährdung. Die Schwachstelle kann unter Umständen ausgenutzt werden, um IOS XE Systeme aus der Ferne zu kompromittieren, die dann als Weg in interne Netzwerke dienen könnten.

Das aktuelle Fehlen eines verfügbaren Patches für die Schwachstelle CVE-2023-20198 ist besonders schwerwiegend, da es anderweitige Mitigationsmaßnahmen von IT-Sicherheitsveranwortlichen erfordert. Korrekt konfigurierte IOS XE Systeme, die nicht aus dem Internet erreichbar sind, sind zumindest vor Angriffen von extern geschützt.

Durch die Verfügbarkeit von Indikatoren zum Prüfen auf eine mögliche Kompromittierung (IoCs) kann eine möglicherweise bereits erfolgte Ausnutzung detektiert werden.

Update 1:
Die beobachtete breitflächige Ausnutzung macht eine bereits stattgefundene Kompromittierung wahrscheinlich und eine Überprüfung des Cisco IOS XE Geräts notwendig.

Update 2:
Mit den verfügbaren Patches ist eine Schließung der Schwachstellen CVE-2023-20198 und CVE-2023-20273 nun ohne Workaround möglich, es bleibt jedoch, auf eine bereits stattgefundene Kompromittierung zu prüfen.

Maßnahmen

IT-Sicherheitsverantwortliche sollten schnellstmöglich für ihre Cisco IOS XE Instanzen **prüfen, ob** diese **die Weboberfläche aktiviert** haben und falls dies der Fall ist, sicherstellen, dass diese nur aus vertrauenswürdigen Netzwerken erreichbar oder deaktiviert ist. Ob die Weboberfläche aktiviert ist, kann folgendermaßen geprüft werden [CISCO23]:

- Sollte der Befehl ***show running-config | include ip http server|secure|active*** auf dem IOS XE Systemzur Ausgabe "*ip http server*" oder/und "*ip http secure-server*" führen, so ist die Weboberfläche aktiv und das System durch die Schwachstelle gefährdet.

Beispiel:

```
Router# show running-config | include ip http server|secure|active
ip http server
ip http secure-server
```

- Sollte "*ip http server*" aktiviert sein, die Konfiguration jedoch auch "*ip http active-session-modules none*" enthalten, so ist diese Schwachstelle nicht über HTTP ausnutzbar.
- Sollte "*ip http secure-server*" aktiviert sein, die Konfiguration jedoch auch "*ip http secure-active-session-modules none*" enthalten, so ist die Schwachstelle nicht über HTTPS ausnutzbar.

Cisco gibt im Advisory ebenfalls Indikatoren (IoCs) zur Detektion einer möglicherweise bereits stattgefundenen Kompromittierung an [CISCO23].

- Systemlogs sollten auf Einträge geprüft werden, welche den Nutzer "*cisco_tac_admin*", "*cisco_support*" oder einen anderen für den Administrator unbekannten Nutzernamen enthalten. Siehe Beispiele, wobei "user" für einen der Nutzernamen steht:

```
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as user on line
%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: user] [Source: source_IP_address] at 03:42:13 UTC Wed Oct 11 2023
```

Hinweis: Der Eintrag "%SYS-5-CONFIG_P" wird immer dann angezeigt, wenn ein Nutzer auf die Weboberfläche zugreift. Es sollte daher auf neue bzw. unbekannte Nutzernamen geprüft werden.

- Systemlogs sollten auf Einträge geprüft werden, die Installations-Aktionen von unbekannten Dateien (identifizierbar an den Dateinamen, hier "filename") enthalten. Siehe Beispiel:

```
%WEBUI-6-INSTALL_OPERATION_INFO: User: username, Install Operation: ADD filename
```

- Mithilfe eines von Cicso Talos [TALOS23] bereitgestellten Befehls kann das Vorhandensein einer Infektion des Systems geprüft werden. Hierzu muss folgender Befehl ausgeführt werden, wobei die *systemip* ersetzt werden und das IOS XE System von der ausführenden Workstation erreichbar sein muss. Ggf. muss ebenfalls "*https*" durch "*http*" ersetzt werden:

```
curl -k -X POST "https://systemip/webui/logoutconfirm.html?logon_hash=1"
```

Sollte die Antwort einen hexadezimalen String enthalten, so ist eine Infektion mit der durch Cisco Talos beobachteten Malware wahrscheinlich.

- Die folgenden Snort Regel IDs sind zur Detektion eine Ausnutzung verfügbar:
  - 3:50118:2 - Kann auf eine Initiale Malware Infektion hindeuten
  - 3:62527:1 - Kann auf eine Malware Interaktion hindeuten
  - 3:62528:1 - Kann auf eine Malware Interaktion hindeuten
  - 3:62529:1 - Kann auf eine Malware Interaktion hindeuten
- In einem Beitrag von Cisco Talos [TALOS23] werden die IPs 5.149.249[.]74 und 154.53.56[.]231 angegeben, von denen beobachtete Angriffe ausgingen. Des Weiteren enthält der Beitrag Details zum Ablauf der beobachteten Angriffe auf die Weboberfläche von Cisco IOS XE.

Update 1:
Cisco Talos hat weitere IoCs in ihrem Blogbeitrag [TALOS23] hinzugefügt:

- IP-Adresse: 154.53.63[.]93
- Nutzername: cisco_sys_manager
- Die Snort Regel IDs für initiale Ausnutzung von CVE-2023-20198: 3:62541 und 3:62542
- Die Snort Regel 3:50118 verweist auf eine Malware Infektion durch CVE-2021-1435

Cisco Talos hat beobachtet, dass die Angreifenden Nutzer und Logs löschen mit folgenden Befehlen [TALOS23]:

```
clear logging
no username cisco_support
no username cisco_tac_admin
no username cisco_sys_manager
```

Orange Cyberdefence hat auf GitHub [GITH23] ein Skript veröffentlicht, dass mittels einer IP-Adresse von einem Cisco IOS XE Gerät auf eine mögliche Kompromittierung auf CVE-2023-20198 prüft.

Es ist wichtig, dass verdächtige Accounts (Administratoren - Level 15) gelöscht werden, da ansonsten weiterhin der Zugriff für die Angreifenden auf die Cisco IOS XE Geräte besteht, auch nach dem Entfernen der Malware. Die aktuell beobachtete Malware ist nicht persistent und wird durch einen Neustart des Gerätes entfernt. [TALOS23]

Update 2:
Der jeweilige Patch zum Beheben der Schwachstellen sollten zeitnah eingespielt werden (Verfügbarkeitsstatus findet sich im Advisory [CISCO23]. Folgende Patch-Versionen beheben die Schwachstellen:

- 17.9.4a
- 17.6.6a
- 17.3.8a
- 16.12.10a

Nach dem Einspielen des Patches sollte auf eine Kompromittierung mittels obiger Maßnahmen geprüft werden. Die Weboberfläche sollte jedoch als generelle Empfehlung weiterhin nur aus vertrauenswürdigen Netzwerken erreichbar sein.

Korrektur:

- Die Snort Regel 3:50118 verweist nach neuem Kentnissstand nicht auf eine Malware Infektion durch CVE-2021-1435 sondern mittels CVE-2023-20273 hin. [TALOS23]

Update 3:
Durch die Aktualisierung der Malware durch die Angreifenden funktioniert die Erkennung mittels einer HTTP-Anfrage auf "*https://systemip/webui/logoutconfirm.html?logon_hash=1*" nicht mehr.

Jedoch konnte eine neue Erkennung mittels des Pfades "*https://systemip/%25*" durch die IT-Sicherheitsforschenden von Fox-IT ermittelt werden. Fox-IT stellt ebenfalls ein Python-Script zur Verfügung, mit dem Cisco IOS XE Geräte auf eine mögliche Malware-Infektion geprüft werden können. Im Falle einer Malware-Infektion sollte die Antwort "*<head><title>404 Not Found</title></head>*" enthalten. [GITH23]

Ein Installieren des Updates und Neustart entfernt die Malware, jedoch nicht möglicherweise von den Angreifenden angelegte Zugänge (Accounts). Die verfügbaren Patches finden sich im Advisory [CISCO23].

IT-Sicherheitsverantwortliche sollten - solange kein Patch zur Verfügung steht - das HTTP Server Feature auf allen aus dem Internet erreichbaren IOS XE Systemen deaktivieren. Dazu muss "*no ip http server*" oder/und "*no ip http secure-server*" im globalen Konfigurationsmodus als Befehl ausgeführt werden. Damit die Änderung auch nach einem Neustart erhalten bleibt, sollte "*copy running-configuration startup-configuration*" ausgeführt werden, um die aktuelle Konfiguration abzuspeichern. Ebenfalls sollte mithilfe der oben genannten Prüfmethode sichergestellt werden, dass die HTTP/HTTPS Funktionalität tatsächlich nicht mehr aktiviert ist.

Cisco hat zusätzlich einen Entscheidungsbaum für IT-Sicherheitsverantwortliche erstellt, der genutzt werden kann, um die Handlungsnotwendigkeit zu prüfen [CISCO23]:

- Wird IOS XE eingesetzt?
  - **Nein**. Keine verwundbaren Systeme.
  - **Ja**. Ist ***ip http server*** oder ***ip http secure-server*** aktiviert?
    - **Nein**. Keine weiteren Aktionen notwendig, die Schwachstelle ist nicht ausnutzbar.
    - **Ja**. Laufen Dienste, die HTTP/HTTPS Kommunikation benötigen (z.B. eWLC)?
      - **Nein**. Deaktivieren Sie das HTTP Server Feature.
      - **Ja**. Wenn möglich, den Zugriff auf das System auf vertrauenswürdige Netzwerke beschränken.

Bis ein Patch verfügbar ist, sollte regelmäßig das Advisory [CISCO23] gesichtet werden, um die Verfügbarkeit von Patches oder weiteren Indikatoren einer Kompromittierung zeitnah wahrnehmen zu können. Cisco bietet einen Leitfaden an, wie IOS XE Systeme generell gehärtet werden können [CISCOdocs].

Links

[CISCO23] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

[CISCOdocs] https://www.cisco.com/c/de_de/support/docs/ios-nx-os-software/ios-xe-16/220270-use-cisco-ios-xe-hardening-guide.html

[TALOS23] https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

Update 1:
[CENS23] https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday/

[ROCK23] https://www.rockwellautomation.com/fr-ch/support/advisory.PN1653.html

[GITH23] https://github.com/cert-orangecyberdefense/Cisco_CVE-2023-20198

Update 2:
[BLEE23] https://www.bleepingcomputer.com/news/security/number-of-hacked-cisco-ios-xe-devices-plummets-from-50k-to-hundreds/

Update 3:
[GITH23] https://github.com/fox-it/cisco-ios-xe-implant-detection

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

    TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
    Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.