Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Cisco ASA: Aktiv ausgenutzte Schwachstellen geschlossen

CSW-Nr. 2024-232160-1032, Version 1.0, 24.04.2024

IT-Bedrohungslage*: 3 / Orange

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 24. April 2024 veröffentlichte der Hersteller Cisco drei Advisories [CISC24a], [CISC24b], [CISC24c] zu Schwachstellen in seinem Produkt Cisco ASA (Adaptive Security Appliance).

Auslöser waren Beobachtungen, wonach zwei der Verwundbarkeiten bereits in gezielten Attacken verwendet werden:
Die Schwachstelle mit der Kennung CVE-2024-20359 versetzt einen lokalen Angreifenden in die Lage, mit hohen Berechtigungen Code ausführen zu können. In diesem Zusammenhang wurde bereits die Platzierung von persistenten Webshells durch die Täter entdeckt. Gemäß Common Vulnerability Scoring System (CVSS) erhält die Sicherheitslücke eine Bewertung von 6.0 (mittlere Kritikalität).

CVE-2024-20353 ermöglicht Denial-of-Service Attacken aus der Ferne und wurde nach CVSS mit 8.6 (hohe Kritikalität) bewertet.

Mit der Command-Injection Schwachstelle CVE-2024-20358 wurde außerdem eine weitere Verwundbarkeit bekannt, deren CVSS-Score bei 6.0 liegt. Hinweise auf eine Ausnutzung liegen Cisco zum aktuellen Zeitpunkt jedoch nicht vor.

Die betroffenen Produktversionen und -konfigurationen variieren mit den genannten Schwachstellen. Details können [CISC24a], [CISC24b] und [CISC24c] entnommen werden. In allen drei Fällen sind jedoch sowohl ASA Lösungen mit dem Betriebssystem ASA Software als auch mit Firepower Threat Defense (FTD) verwundbar.

* 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.

Den Veröffentlichungen vorangegangen waren Untersuchungen von Ciscos Product Security Incident Response Team (PSIRT) sowie der Threat Intelligence Sparte des Unternehmens, Cisco Talos, nachdem diese im Januar 2024 Hinweise auf den Sachverhalt erhalten hatten. In Kooperation mit mehreren internationalen Partnern ergaben die Analysen, dass Täter mithilfe einer sehr ausgefeilten Angriffsvariante in der Lage waren, eine kleine Anzahl an Systemen bei Kunden zu kompromittieren und Daten zu exfiltrieren. Betroffen waren Behörden und Unternehmen aus den Kritischen Infrastrukturen auf der ganzen Welt [TALO24] [CACE24]. Weiterhin bezeichnete Cisco Talos die Kampagne als "ArcaneDoor".

Das britische NCSC-UK veröffentlichte ebenfalls Analysen über die von dem Akteur genutzten Schadsoftware-Varianten. Demnach wurde ein Shellcode Loader "Line Dancer" [NCSC24a] sowie eine persistente Webshell "Line Runner" [NCSC24b] eingesetzt, die sehr ausgefeilt Detektionsmechanismen umgeht und sicherstellt, dass lediglich der Akteur Befehle auf kompromittierten Geräten ausführen kann.

Nach dem Bericht [NCSC24a] wurde der in-memory Shellcode Loader bereits Ende 2023 und Anfang 2024 in Angriffen gegen Cisco ASA Geräte in Verbindung mit der "ArcaneDoor " Kampagne eingesetzt. Es wurde beobachtet, dass "Line Dancer" kombiniert mit der Webshell "Line Runner" genutzt wurde.

Bei der zweiten beobachteten Schadsoftware-Variante "Line Runner" handelt es sich um eine persistente Webshell, die schwierig zu detektieren ist und nicht durch einen Neustart des Gerätes entfernt werden kann. Die Webshell ermöglicht die Auführung von Lua Code und unterscheidet sich von "Line Dancer". [NCSC24b]

Es ist bislang unklar, wie die Schadsoftware-Varianten auf Cisco ASA Geräten platziert werden konnten. Möglicherweise durch die Nutzung von Zugangsdaten oder mithilfe einer Schwachstelle. Bislang konnte Cisco jedoch keine Hinweise finden, die auf eine Schwachstelle hindeuten, die das Umgehen der Authentifizierung ermöglicht. [TALO24]

Bewertung

Firewalls und VPN-Gateways sind für die Sicherheit von IT-Netzwerken von zentraler Bedeutung. Möglicherweise darin vorhandene Schwachstellen stellen somit grundsätzlich massive Gefährdungen für Institutionen und Privatpersonen dar. Eine Kompromittierung bietet zahlreiche Optionen zur Ausbreitung auf interne Netzwerke und zur Manipulation des Datenverkehrs.

Mit mehr als 6.000 öffentlich auffindbaren Geräten in Deutschland ist die hier verwundbare Cisco ASA Firewall daher ein attraktives Ziel für Cyber-Angriffe. Selbst wenn bislang ausschließlich gezielte Attacken bekannt sind, muss davon ausgegangen werden, dass die Täter ihre Angriffsversuche nach dem öffentlichen Bekanntwerden der Schwachstellen in kurzer Zeit auch großflächig ausdehnen. Die Umsetzung von Schutzmaßnahmen ist daher für alle Betreiber ratsam – unabhängig von den bislang im Fokus stehenden Branchen.

Die nach CVSS zum Teil "nur" mit mittlerer Kritikalität bewerteten Schwachstellen sollten IT-Sicherheitsverantwortliche gleichzeitig nicht dazu verleiten, die Umsetzung dieser Maßnahmen herab zu priorisieren.

Maßnahmen

IT-Sicherheitsverantwortliche sollten unverzüglich die zur Verfügung stehenden Patches [CISC24a], [CISC24b], [CISC24c] installieren und auf eine mögliche, bereits stattgefundene Kompromittierung prüfen.

Zur Detektion von Angriffen mittels CVE-2024-20353 und CVE-2024-20359 hat Cisco IOCs veröffentlicht. Hierzu zählt insbesondere der Abgleich ein- und ausgehender Verbindungen von/zu den unter [TALOS24] genannten IP-Adressen. Sollten Hinweise auf derartige Verbindungen vorliegen und die Crash Dump-Funktionalität an den betroffenen Geräten verändert worden sein, bittet Cisco darum, ein Ticket beim Kundensupport zu öffnen.

Detektion "Line Dancer"

Es wird empfohlen die Detektion von "Line Dancer" **vor dem Einspielen der Patches oder der Prüfung auf die Webshell "Line Runner" durchzuführen**, da nach einem Geräte-Neustart jegliche Indikatoren sowie die Schadware selbst verschwinden.

Die Ausgabe des Befehls "*show memory region | Include lina*" (im Enable Mode) kann genutzt werden, um die Präsenz von "Line Dancer" festzustellen. Sollte mehr als ein gelisteter Speicherbereich mit der Executable Flag (x) bzw. mit dem

Berechtigungen "*r-xp*" gekennzeichnet sein und eine Speicherregion die Größe 0x1000 besitzen, so ist das Gerät kompromittiert. [TALO24][NCSC24a]

Ein Beispiel sowie eine Yara-Regel zur Detektion finden sich ebenfalls in der Malware-Analyse von NCSC-UK.

Detektion "Line Runner"

Zur Detektion der Webshell "Line Runner" stehen mehrere Möglichkeiten zur Verfügung, die jedoch alle einen Neustart des Geräts erfordern.

Nach der Aktualisierung des Geräts sollte der Inhalt von disk0: geprüft werden. Sollte eine neue Datei (z.B. “client_bundle_install.zip” oder andere ungewöhnliche .zip Dateien) erscheinen, so deutet dies auf die "Line Runner" Schadware hin. Durch das Einspielen des Patches [CISC24c] ist diese jedoch nicht länger auf dem Gerät aktiv. [TALO24]

Eine weitere Möglichkeit ohne Einspielen des Patches (nicht empfohlen) besteht darin, eine Datei, welche dem Lua Muster *^client_bundle[%w_-]%.zip$* entspricht, selbst im *disk0:* Ordner anzulegen. Dies sorgt dafür, dass die Schadware beim Neustart des Geräts einen Fehler verursacht und gleichzeitig vom Gerät entfernt wird. Das Resultat ist, dass der Neustart der Cisco ASA die selbst-erstellte Datei löschen und mit der schadhaften ZIP-Datei austauschen wird. Nach dem Neustart kann durch das Ausführen des Befehls "*show disk0:*" festgestellt werden, ob eine Kompromittierung stattgefunden hat. Sollte die Datei client_bundle_install.zip existieren, so zeigt dies eine Kompromittierung. Die angezeigte ZIP-Datei ist in diesem Fall die "Line Runner" Schadware [NCSC24b].

Ebenfalls ist es möglich, über traditionelle forensische Untersuchung des Datenträgers eine Kompromittierung festzustellen. Diese Option benötigt jedoch physikalischen Zugang auf den Speicher, wird nicht von Cisco empfohlen und sorgt dafür, dass das Gerät nicht mehr vom Hersteller unterstützt wird [NCSC24b]!

Mehr Informationen zur Detektion von "Line Runner" kann bei NCSC-UK [NCSC24b] gefunden werden.

Darüber hinaus veröffentlichte Cisco Snort Signaturen, mit denen eine Ausnutzung bzw. die Schadware festgestellt werden kann [TALO24]:

- CVE-2024-20353 (ASA DOS/Reboot) - 3:63139
- "Line Runner" – Persistence Mechanism Interaction – 3:62949
- "Line Dancer" – In-Memory Only Shellcode Interpreter Interaction – 3:45575

Weitere Hinweise zur sicheren Nutzung von Firewalls können dem BSI IT-Grundschutz [BSIG24] entnommen werden.

Links

[CISC24a] Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services Denial of Service Vulnerability – CVE-2024-20353:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

[CISC24b] Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability – CVE-2024-20358:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm

[CISC24c] Cisco Adaptive Security Appliance and Firepower Threat Defense Software Persistent Local Code Execution Vulnerability - CVE-2024-20359:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

[TALO24] Cisco Talos Blog - "ArcaneDoor " new espionage focused campaign found targeting perimeter network devices:
https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

[CACE24] Cyber Activity Impacting CISCO ASA VPNs:
https://www.cyber.gc.ca/en/news-events/cyber-activity-impacting-cisco-asa-vpns

[NCSC24a] NCSC-UK - Line Dancer Malware Analysis:
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/line/ncsc-tip-line-dancer.pdf

[NCSC24b] NCSC-UK - Line Runner Malware Analysis:
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/line/ncsc-tip-line-runner.pdf

[BSIG24] BSI IT-Grundschutz: NET.3.2 Firewall (Edition 2023):
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2023.html

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.