Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Proof-of-Concept Exploit veröffentlicht für Schwachstellen in Juniper Firewalls und Switches

CSW-Nr. 2023-258036-1132, Version 1.1, 19.09.2023

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 25. August veröffentlichte watchTowr eine detaillierte technische Beschreibung sowie ein Proof-of-Concept (PoC) Exploit für Schwachstellen in Junos OS - der SRX (Firewalls) und EX (Switches) Serie von Juniper [WATCH23]. Die Inhalte zielen auf Verwundbarkeiten in der Komponente J-Web ab, die der Hersteller erst am 17. August bekanntgegeben hat [JUNIP23]. Juniper stellt bislang noch nicht für alle betroffenen Versionen Patches bereit. Die Sicherheitslücken erlauben einem Angreifenden ohne Authentifizierung die Ausführung von Code~~, wenn diese kombiniert ausgenutzt werden~~. Alle vier geschlossenen Schwachstellen werden mit einem CVSS von 5.3 ("mittel") bewertet, kombiniert sollen sie allerdings laut Juniper Networks einen Score von 9.8 ("kritisch") erreichen.

Update 1:
Am 18. September veröffentlichte VulnCheck [VULN23] einen Blog Beitrag, in dem ein Proof-of-Conept Exploit vorgestellt wird, welches eine Ausführung von Code ohne Authentifizierung alleinig durch die Ausnutzung von CVE-2023-36845 ermöglicht. Die Code-Ausführung wird hierbei ohne das Erstellen einer Datei auf dem System durch die Manipulation von Umgebungsvariablen umgesetzt, weshalb gegenüber dem am 25. August veröffentlichten PoC die Schwachstellen nicht mehr kombiniert ausgenutzt werden müssen.

* 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.

CVE-2023-36844 und CVE-2023-36845

- Ermöglichen es einem netzwerkbasierten Angreifenden, wichtige Umgebungsvariablen ohne Authentifizierung zu verändern.

CVE-2023-36846 und CVE-2023-36847

- Versetzen Angreifende dazu in die Lage, mit einer spezifischen Anfrage ohne Authentifizierung beliebige Dateien über J-Web hochzuladen, was zu einem Verlust der Integrität für einen bestimmten Teil des Dateisystems führt.

Update 1:
CVE-2023-36851

- Versetzt Angreifende dazu in die Lage, mit einer spezifischen Anfrage ohne Authentifizierung beliebige Dateien über J-Web auf SRX Firewalls hochzuladen, was zu einem Verlust der Integrität für einen bestimmten Teil des Dateisystems führt.

Die Schwachstelle wurde im September im Security Advisory von Juniper [JUNIP23] aufgenommen.

Die Schwachstellen betreffen folgende Produkte:

Juniper Networks Junos OS der SRX Serie (Firewalls):

- Alle Versionen vor 20.4R3-S8
- 21.1 Versionen ab 21.1R1 und höher
- 21.2 Versionen vor 21.2R3-S6
- 21.3 Versionen vor 21.3R3-S5
- 21.4 Versionen vor 21.4R3-S5
- 22.1 Versionen vor 22.1R3-S3
- 22.2 Versionen vor 22.2R3-S2
- 22.3 Versionen vor 22.3R2-S2, 22.3R3
- 22.4 Versionen vor 22.4R2-S1, 22.4R3

Juniper Networks Junos OS der EX Serie (Switches):

- Alle Versionen vor 20.4R3-S8
- 21.1 Versionen ab 21.1R1 und höher
- 21.2 Versionen vor 21.2R3-S6
- 21.3 Versionen vor 21.3R3-S5
- 21.4 Versionen vor 21.4R3-S4
- 22.1 Versionen vor 22.1R3-S3
- 22.2 Versionen vor 22.2R3-S1
- 22.3 Versionen vor 22.3R2-S2, 22.3R3
- 22.4 Versionen vor 22.4R2-S1, 22.4R3

Junos OS Version 21.1 ist End of Engineering (EoE) und wird daher keinen Patch zum Schließen der Schwachstelle erhalten.

Bewertung

Firewalls stellen aufgrund ihrer zentralen Bedeutung als Schutzsystem und ihrer exponierten Position für die IT in Organisationen attraktive Ziele für Cyber-Angriffe dar. Eine Kompromittierung bietet zahlreiche Optionen zur weiteren Ausbreitung in internen Netzwerken und zur Manipulation des Datenverkehrs.

Mit der Veröffentlichung des PoC-Exploits [WATCH23][VULN23] ist die Ausnutzung der Schwachstellen nun einfach möglich. Angreifende können ohne Authentifizierung Code einschleusen und so Firewalls und Switches kompromittieren sowie Zugang zum geschützten Netzwerkbereich erhalten.

Auf Grund der öffentlichen technischen Details ist eine zeitnahe Ausnutzung der Schwachstellen in den betroffenen Junos OS Versionen zu erwarten. ~~Aktuell gibt es allerdings noch keine Erkenntnisse über bereits stattfindende Angriffe~~, Patches sollten jedoch zur Gewährleistung der Sicherheit schnellstmöglichst installiert werden.

Update 1:
Im Beitrag von VulnCheck [VULN23] wird von Shadowserver und GreyNoise erkannten versuchten Angriffen mittels des PoC Exploits von watchTowr berichtet. Des Weiteren geht aus dem Blog Beitrag hervor, dass ca. 80% der weltweit über 15.000 gefundenen Juniper Firewalls nicht gepatcht wurden. Diese Erkenntnis wurde mittels eines bereitgestellten Scripts [GITH23] erlangt, welches genutzt werden kann, um auf die Betroffenheit von CVE-2023-36845 zu prüfen.

Maßnahmen

IT-Sicherheitsverantwortliche sollten kurzfristig die Verfügbarkeit und Installation der vom Hersteller bereitgestellten Patches prüfen. Diese sind

- für die EX Serie:
  - Veröffentlichungen aus dem Problem Report (PR) 1735387 mit den Junos OS-Versionen: 20.4R3-S8, 21.2R3-S6, 21.3R3-S5*, 21.4R3-S4, 22.1R3-S3, 22.2R3-S1, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3*, 23.2R1 und alle späteren Versionen
- für die SRX Serie:
  - Veröffentlichungen aus dem Problem Report (PR) 1735389 mit den Junos OS-Versionen: 20.4R3-S8, 21.2R3-S6, 21.3R3-S5*, 21.4R3-S5*, 22.1R3-S3, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3*, 23.2R1 und alle späteren Versionen.

Update 1:
Für die SRX Serie steht ein weiterer Problem Report (PR) 1736942 mit den Junos OS Versionen: 20.4R3-S9*, 21.2R3-S7*, 21.3R3-S5*, 21.4R3-S5*, 22.1R3-S4*, 22.2R3-S2, 22.3R2-S2, 22.3R3-S1*, 22.4R2-S1, 22.4R3*, 23.2R1-S1, 23.2R2*, 23.4R1* und allen späteren Versionen zur Verfügung. Dieser betrifft die später aufgenommene Schwachstelle CVE-2023-36851. Zu dieser Schwachstelle gibt es kein PoC Exploit oder eine bekannte Ausnutzung.

Die Veröffentlichung von mit * gekennzeichneten Releases wird derzeit noch durch den Hersteller vorbereitet. Das BSI empfiehlt Betreibern von betroffenen Geräten daher, regelmäßig die Verfügbarkeit der momentan noch nicht abrufbaren Patches zu prüfen.

Details zu den genannten Problem Reports sind ebenfalls auf der Juniper-Webseite zu finden, erfordern jedoch einen Kundenlogin.

Sofern eine Installation der Patches (noch) nicht möglich ist, empfiehlt Juniper als Workaround, J-Web vollständig abzuschalten oder zumindest den Zugriff nur auf vertrauenswürdige IP-Adressen einzuschränken.

Zur Sicherstellung der Integrität der Systeme bzw. zum Ausschluss einer bereits erfolgten Kompromittierung können PHP Logs laut watchTowr [WATCH23] auf folgende Einträge geprüft werden:

```
[...] Array(
  [type] => 8
  [message] => Trying to access array offset on value of type null
  [file] => /html/core/session.php
  [line] => 47
)
```

Diese Fehlermeldung entsteht nur bei anonymen Zugriff ohne valide Session und deutet auf eine stattgefundene Ausnutzung hin.

```
[...] CACHING FLOW: query user not set.
```

Bei diesem Eintrag handelt es sich um einen Fehler der auftritt, falls auf einen API-Endpunkt ohne Authentifizierung zugegriffen werden sollte. Dies sagt zwar nicht aus, dass eine erfolgreiche Ausnutzung stattgefunden hat, kann jedoch ein Indikator dafür sein, dass Angreifende die Möglichkeiten der API testen.

Update 1:
Laut VulnCheck [VULN23] sollte der httpd-Log auf Einträge geprüft werden wie:

> httpd: 2: POST /?PHPRC=/dev/fd/0 HTTP/1.1

Der Angreifer kann jedoch ebenso auf Variablen im HTTP-Header verzichten, wodurch keine eindeutigen Indikatoren auf Angriffe mehr in den httpd-Logs erscheinen.

Links

[JUNIP23] https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution

[WATCH23] https://labs.watchtowr.com/cve-2023-36844-and-friends-rce-in-juniper-firewalls/

[VULN23] https://vulncheck.com/blog/juniper-cve-2023-36845

[GITH23] https://github.com/vulncheck-oss/cve-2023-36845-scanner

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.