



| **Flash** |

Active Exploitation of Juniper RCE Vulnerabilities

F-2023-11-17a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Vulnerability Exploitation, Malware, Deep Dark Web & Criminal Underground

November 17, 2023

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on November 17, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Active Exploitation of Juniper RCE Vulnerabilities

› Key Findings

- On November 13, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) added five Juniper Junos operating system (OS) vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog based on evidence of active exploitation.
- A recent Proof-of-Concept (PoC) for four of the vulnerabilities demonstrated how an unauthenticated, network-based threat actor may be able to remotely execute malware on unpatched assets by chaining exploitation of these vulnerabilities.
- Threat actors' increased adoption of the vulnerability chaining technique poses a complex cyber threat to organizations with unpatched internet-facing assets.
- Based on the availability of PoC exploits, which lower the barriers to entry for exploiting these vulnerabilities, ZeroFox assesses these vulnerabilities to be critical as a collective because threat actors are likely to exploit them on unpatched assets in the long term, potentially leading to widespread exploitation.
- ZeroFox anticipates that threat actors are very likely to create their own customized PoC exploits and sell them on darknet forums.

| Details

On November 13, 2023, CISA added five Juniper Junos OS vulnerabilities to its KEV Catalog based on evidence of active exploitation.

CVE	Description	CVSS v3.x ¹	Severity
CVE-2023-36844	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	5.3	Medium
CVE-2023-36845	Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability	N/A	N/A
CVE-2023-36846	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	N/A	N/A
CVE-2023-36847	Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability	N/A	N/A
CVE-2023-36851	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability ²	5.3	Medium

Table 1. Actively Exploited Juniper OS Vulnerabilities

Sources: CISA and NVD

As of November 16, 2023, there were over 10,000 internet-facing assets with vulnerable Juniper J-Web interfaces. The United States had the second highest number of vulnerable internet-facing assets (1,215).³

¹ Analyst note: N/A for CVSS v3.x indicates that a CVSS score/severity for this CVE has not been published yet.

² [hXXps://www.cisa\[.\]gov/news-events/alerts/2023/11/13/cisa-adds-six-known-exploited-vulnerabilities-catalog](https://www.cisa.gov/news-events/alerts/2023/11/13/cisa-adds-six-known-exploited-vulnerabilities-catalog)

³

[hXXps://dashboard.shadowserver\[.\]org/statistics/iot-devices/time-series/?date_range=90&vendor=juniper&model=web+device+manager&group_by=geo&style=stacked](https://dashboard.shadowserver[.]org/statistics/iot-devices/time-series/?date_range=90&vendor=juniper&model=web+device+manager&group_by=geo&style=stacked)

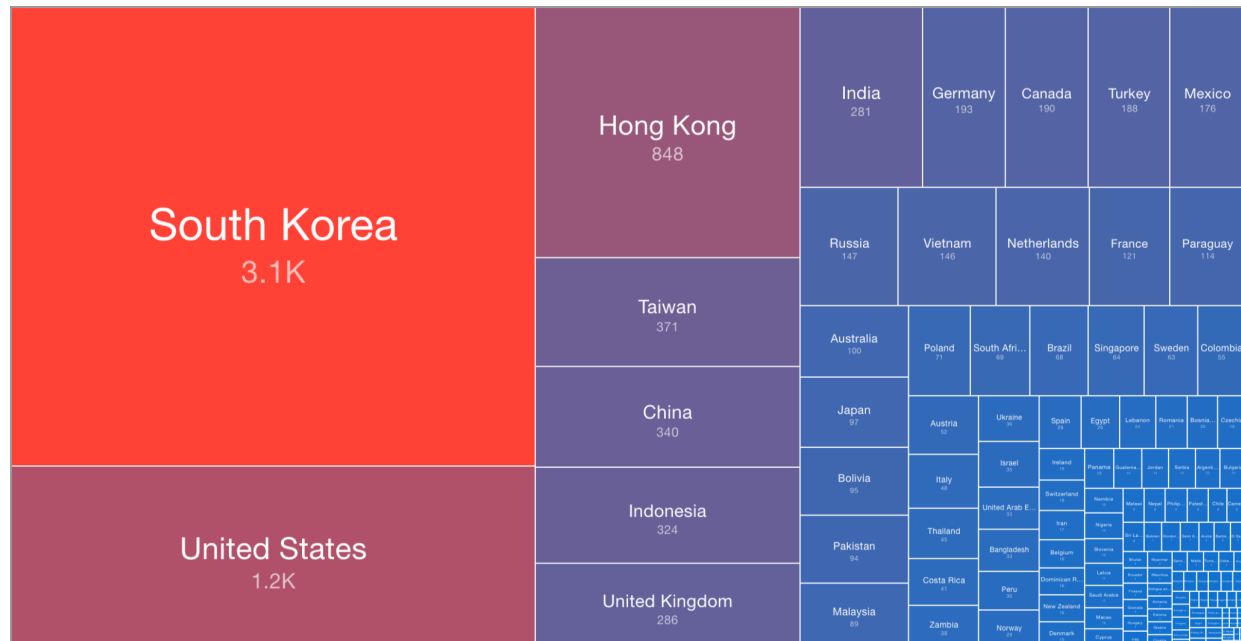


Figure 1. Vulnerable Juniper Internet-Facing Assets by Country and Count

Source:

[https://dashboard.shadowserver\[.\]org/statistics/iot-devices/tree/?day=2023-11-16&vendor=juniper&model=web+device+manager&geo=all&data_set=count&scale=log](https://dashboard.shadowserver[.]org/statistics/iot-devices/tree/?day=2023-11-16&vendor=juniper&model=web+device+manager&geo=all&data_set=count&scale=log)

Analyst Commentary

A PoC for four of the vulnerabilities in Table 1 (CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, and CVE-2023-36847)⁴ was published by cybersecurity firm watchTowr Labs when they were first disclosed by Juniper in August 2023.⁵ The PoC demonstrates how an unauthenticated, network-based threat actor may be able to conduct remote code execution (RCE) on unpatched assets by chaining exploitation of these vulnerabilities.⁶ RCE vulnerabilities, a subclass of arbitrary code execution (ACE)

⁴

[https://github\[.\]com/watchtowrlabs/juniper-rce_cve-2023-36844#cve-2023-36844--cve-2023-36845--cve-2023-36846--cve-2023-36847](https://github[.]com/watchtowrlabs/juniper-rce_cve-2023-36844#cve-2023-36844--cve-2023-36845--cve-2023-36846--cve-2023-36847)

⁵ [https://labs.watchtowr\[.\]com/cve-2023-36844-and-friends-rce-in-juniper-firewalls/](https://labs.watchtowr[.]com/cve-2023-36844-and-friends-rce-in-juniper-firewalls/)

⁶

[https://www.bleepingcomputer\[.\]com/news/security/cisa-warns-of-actively-exploited-juniper-pre-auth-rce-exploit-chain/](https://www.bleepingcomputer[.]com/news/security/cisa-warns-of-actively-exploited-juniper-pre-auth-rce-exploit-chain/)

vulnerabilities, are one of the most dangerous classes of vulnerabilities because their exploitation could allow threat actors to execute malware on a remote machine.⁷

Moreover, this PoC highlights vulnerability chaining, a threat actor tradecraft technique that occurs during the reconnaissance phase. While enumerating a target's digital footprint, threat actors identify direct and peripheral vulnerabilities and flaws in software/hardware to exploit.⁸ Using this iterative approach, threat actors can breach an organization's defenses and gain unauthorized access to its systems. Vulnerability chaining poses a significant risk to organizations with unpatched internet-facing assets because it can neutralize cybersecurity measures and exploit known vulnerabilities. Vulnerability chaining is especially a risk for organizations with unpatched internet-facing assets due to:

1. **Cumulative impact:** While a single unpatched vulnerability may not pose a significant threat on its own, its impact can be magnified when combined with other vulnerabilities via chaining. Multiple vulnerabilities can be exploited by threat actors to gain deeper access into an organization's systems, potentially resulting in data breaches, service disruptions, or unauthorized control.
2. **Expanded attack surface:** Unpatched internet-facing assets expand an organization's attack surface, giving threat actors more opportunities to find vulnerabilities and launch an attack.
3. **Increased exploitation risk:** Vulnerability chaining enables threat actors to exploit dependencies between vulnerabilities. They can infiltrate an organization's network using a combination of exploits and techniques such as privilege escalation, lateral movement, or pivoting. This increases the likelihood of successful exploitation, especially if the vulnerabilities are relatively simple to exploit or if there are already available exploits in the wild.
4. **Privilege escalation:** Vulnerability chaining allows threat actors to gain access to higher-level resources within an organization's network. They can attain greater access privileges by exploiting multiple vulnerabilities in succession, potentially gaining access to critical systems or sensitive data. This can result in further

⁷ [hXXps://socradar\[.\]io/the-most-dangerous-of-their-kind-remote-code-execution-rce-attacks/](https://socradar[.]io/the-most-dangerous-of-their-kind-remote-code-execution-rce-attacks/)

⁸ [hXXps://libertyadvisorgroup\[.\]com/insight/cyber-update-vulnerability-chaining/](https://libertyadvisorgroup[.]com/insight/cyber-update-vulnerability-chaining/)

compromise, data theft, or other malicious activities—all of which can have serious consequences for the organization.

In addition to the vulnerability chaining PoC exploit, threat actors have access to a number of other PoC exploits on the surface web:

PoC Exploit	Description	Author
CVE-2023-36845 PoC Automation Script	This python script automates the PoC for CVE-2023-36845, which targets Juniper Networks Junos OS's J-Web component on EX and SRX Series devices. It exploits a PHP flaw to allow remote change of the PHPRC variable. Exploitation that is successful can result in code injection and execution.	Cyberh3als via GitHub ⁹
CVE-2023-36845 PoC Exploit	This is an instructional guide for exploiting CVE-2023-36845 that contains a Python script, Shodan search terms, Linux commands, and PHP code.	Kljunowsky via GitHub ¹⁰

Table 2. Additional Juniper OS Vulnerabilities PoC Exploits

Source: GitHub

Based on the availability of PoC exploits, which lower the barriers to entry for exploiting these vulnerabilities, ZeroFox assesses these vulnerabilities as a collective to be critical as threat actors are likely to exploit them on unpatched assets in the long term, potentially leading to widespread exploitation.

| Forward Look

ZeroFox assesses that, despite the medium severity level of these vulnerabilities, they may lead to critical cyberattacks and widespread exploitation of unpatched internet-facing assets. This is because these vulnerabilities can be easily exploited without requiring a high skill set. Furthermore, the availability of exploits lowers the barriers to entry for threat actors targeting organizations with unpatched internet-facing assets. Despite the fact that the vulnerabilities were discovered in a next-generation

⁹ [hXXps://github\[.\]com/cyberh3als/CVE-2023-36845-POC](https://github.com/cyberh3als/CVE-2023-36845-POC)

¹⁰ [hXXps://github\[.\]com/kljunowsky/CVE-2023-36845](https://github.com/kljunowsky/CVE-2023-36845)

firewall tool, these types of software vulnerabilities are likely to be targeted attack vectors for threat actors to infiltrate networks and maintain persistence. Furthermore, in terms of the PoC exploits, ZeroFox anticipates that threat actors are very likely to create their own customized PoC exploits and sell them on darknet forums, as has been previously observed.¹¹

| Recommendations

To mitigate the exploitation of these vulnerabilities, organizations should:

- Prioritize patch management for these vulnerabilities.
- Conduct regular vulnerability scans.
- Conduct input validation and data sanitization to mitigate RCE attacks.
- Continuously monitor odd network traffic and suspicious remote connection attempts via remote access tools.
- Utilize secure communication protocols to encrypt data and prevent data tampering to mitigate RCE attacks.
- Implement a defense-in-depth strategy that includes strong firewall rules, intrusion detection systems, and intrusion prevention systems.
- Review access controls and implement the principle of least privilege.
- Implement strong password policies and token-based multi-factor authentication (MFA).
- Utilize the ZeroFox Platform to perform searches on relevant IOCs and monitor for further developments.

¹¹ ZeroFox Internal Intelligence Collections

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%