

CYBER GUIDANCE ISSUE 0406

JUNOS OS VULNERABLE TO RCE

DATE ISSUED: 23rd August 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Juniper Networks, a networking hardware company, has issued an unscheduled security update to fix several vulnerabilities found in the J-Web component of Junos OS. These vulnerabilities could be exploited to enable remote code execution on vulnerable systems.

BREAKDOWN

Several security vulnerabilities have been detected in Junos OS, the operating system used in Juniper's routing, switching, and security devices. When combined in a specific sequence, these vulnerabilities could enable remote code execution. Depending on the privileges linked to the target account, an attacker might install software, manipulate or delete data, or generate new accounts with extensive user privileges. However, service accounts with limited system access likely experience fewer adverse effects than those with administrative rights. The vulnerabilities tracked as [CVE-2023-36844](#) and [CVE-2023-36845](#) are PHP external variable modification vulnerabilities. The two other vulnerabilities tracked, [CVE-2023-36846](#) and [CVE-2023-36847](#), are missing authentications for critical function vulnerabilities. These four combined together have a cumulative rating of CVSS 9.8, making them critical in severity.

REMEDIATION STEPS

- Apply appropriate updates Juniper provides to vulnerable systems immediately after appropriate testing.
- Disable J-Web or limit access to only trusted hosts.
- Enforce strong, unique passwords for each device, using a mix of uppercase and lowercase letters, numbers, and special characters.
- Deploy firewalls and intrusion detection/prevention systems to monitor and filter incoming and outgoing traffic for signs of malicious activity.
- Use multi-factor authentication (MFA) to add an extra layer of security to device access.

REFERENCES & RESOURCES

CIS Advisories https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-junos-os-could-allow-for-remote-code-execution_2023-093

The Hacker News <https://thehackernews.com/2023/08/new-juniper-junos-os-flaws-expose.html>