CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

TLP:CLEAR

12 January 2024

Juno OS Critical Vulnerability

CVE-2024-21591 RCE Juno OS Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-21591.[1] The vulnerability affects J-Web of Juniper Networks Junos OS on SRX Series and EX Series.[2] Exploitation of the vulnerability could allow an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device.[3,4]

Affected Juniper Networks Junos OS SRX Series and EX Series
Junos OS versions earlier than 20.4R3-S9
Junos OS 21.2 versions earlier than 21.2R3-S7
Junos OS 21.3 versions earlier than 21.3R3-S5
Junos OS 21.4 versions earlier than 21.4R3-S5
Junos OS 22.1 versions earlier than 22.1R3-S4
Junos OS 22.2 versions earlier than 22.2R3-S3
Junos OS 22.3 versions earlier than 22.3R3-S2
Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3

Table 1: Vulnerable Junos OS versions

The Cal-CSIC recommends immediately apply the security updates or upgrade JunOS to the appropriate latest release.

For further information on applying upgrades, please refer to Juniper Networks Support Portal.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Bleeping Computer; "Juniper warns of critical RCE bug in its firewalls and switches;" https://www.bleepingcomputer.com/news/security/juniper-warns-of-critical-rce-bug-in-its-firewalls-and-switches/; accessed 12 January 2024

[2] Vulbd; "Juniper Junos Os Up To 22.4r2-S1 On Srx/Ex J-Web Out-Of-Bounds Write;" https://vuldb.com/?id.250502; accessed 12 January 2024

[3] CVE Details; "Vulnerability Details: CVE-2024-21591;" https://www.cvedetails.com/cve/CVE-2024-21591/; accessed 12 January 2024

[4] System Tek; "Critical Remote Code Execution Vulnerability in Junos OS [CVE-2024-21591];" https://www.systemtek.co.uk/2024/01/critical-remote-code-execution-vulnerability-in-junos-os-cve-2024-21591/; accessed 12 January 2024

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.