CYBER ADVISORY

TLP:CLEAR

8 January 2025

Privilege Escalation and OS Command Injection Vulnerabilities in Moxa Devices

CVE-2024-9138 | CVE-2024-9140 | Improper Input | Moxa

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two vulnerabilities known as CVE-2024-9138 and CVE-2024-9140, with a CVSS 3.x score of 7.2[1] and 9.8[2] respectively. Both vulnerabilities affect various Moxa router product series with firmware version prior to 3.14.

Successful abuse of CVE-2024-9138 results in the exploitation of hard-coded credentials that could allow an authenticated user to gain root-level access, leading to system compromise, unauthorized modifications, data exposure, or service disruption. Meanwhile, successful exploitation of CVE-2024-9140, permits operating system (OS) command injection through improper input validation allowing an adversary to execute arbitrary code. There are currently no known instances of either vulnerability being exploited in the wild nor are there any Proof-of-Concepts available.

If updating to the latest version is not possible, as is the case for OnCell G4302 and TN-4900, contact Moxa technical support directly for a security Patch. As for NAT-102 devices, please refer to the mitigation section found in Moxa's Advisory.

The Cal-CSIC recommends immediately updating the affected Moxa routers to firmware version 3.14 or later. For each affected product series refer to its respective firmware update found in the solutions section in Moxa's Advisory.

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] National Vulnerability Database; "CVE-2024-9138 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-9138; accessed 7 January 2025

[2] National Vulnerability Database; "CVE-2024-9140 Detail https://nvd.nist.gov/vuln/detail/CVE-2024-9140; accessed 7 January 2025