Cisco Patches Code and Command Execution Vulnerabilities in Several Products

Cisco this week announced patches for multiple vulnerabilities across its product portfolio, including high-severity issues impacting its Secure Network Analytics and Identity Services Engine (ISE) products.

Tracked as CVE-2023-20102, the first bug is described as insufficient sanitization of user-provided data parsed into memory. An authenticated, remote attacker could send crafted HTTP requests to an affected device to achieve arbitrary code execution.

Cisco has addressed the vulnerability with the release of Secure Network Analytics 7.4.1-Patch SMC Rollup #5.

The tech giant also announced patches for an improper validation of parameters sent to the restricted shell in Cisco ISE, which could lead to privilege escalation.

An authenticated, local attacker could exploit the issue by sending crafted CLI commands, allowing them to escape the restricted shell and gain root privileges on the operating system. Tracked as CVE-2023-20122, the vulnerability was addressed with the release of ISE version 3.2P1.

Cisco’s advisory also details a second improper validation of parameters flaw that impacts the restricted shell of Evolved Programmable Network Manager (EPNM), ISE, and Prime

Infrastructure.

Tracked as CVE-2023-20121, the bug has a severity rating of ‘medium’ because administrator privileges are required for exploitation.

This week, Cisco also announced that a full patch is being released for a critical vulnerability in its Expressway series and TelePresence Video Communication Server (VCS) enterprise collaboration solutions.

Tracked as CVE-2022-20812 (CVSS score of 9.0), the flaw impacts the cluster database API of the affected products and allows an authenticated, remote attacker to overwrite files on the affected device with root privileges, Cisco explains in an advisory.

The issue exists because user-supplied command arguments are not sufficiently validated. To exploit the vulnerability, an attacker needs to authenticate with administrative read-write privileges and submit crafted input.

A partial fix for this vulnerability was included in Expressway series and TelePresence VCS release 14.0.7. A full patch will be included in release 14.3, which is expected to become available in late April.

Cisco also warns of two high-severity vulnerabilities (CVE-2023-20117 and CVE-2023-20128) impacting Small Business RV320 and RV325 routers that could allow an authenticated, remote attacker to execute arbitrary commands on the affected devices.

However, because the affected routers have an end-of-life (EoL) status, Cisco will not release patches to address these vulnerabilities.

No patches will be released for over 15 medium-severity vulnerabilities in EoL Small Business RV016, RV042, RV042G,

RV082, RV320, and RV325 routers either, the tech giant says.

Multiple medium-severity flaws were addressed this week in Cisco Webex Meetings, Unified Contact Center Express (Unified CCX), Secure Network Analytics, Prime Infrastructure and Evolved Programmable Network Manager (EPNM), ISE, Duo Two-Factor Authentication, and Packet Data Network Gateway (PGW).

Cisco says it is not aware of any of these security defects being exploited in attacks. Additional information on these vulnerabilities can be found on Cisco's product security page.

Related: Cisco Patches High-Severity Vulnerabilities in IOS Software

Related: Vulnerability Exposes Cisco Enterprise Routers to Disruptive Attacks

Related: Cisco Patches Critical Vulnerability in IP Phones

Cisco Patches Code and Command Execution Vulnerabilities in Several Products