Cisco Patches Critical Vulnerabilities in Expressway, TelePresence VCS Products

By Ionut Arghire on March 03, 2022

Cisco this week announced patches that address a couple of critical vulnerabilities in its Expressway Series and TelePresence Video Communication Server (VCS) unified communications products.

Tracked as CVE-2022-20754 and CVE-2022-20755 and featuring a CVSS score of 9.0, the two security holes can be exploited by a remote, authenticated attacker to write files or execute code on the underlying operating system with root privileges.

Although they are not dependent on one another, both of the two flaws require that the attacker has read/write privileges to the vulnerable application.

Residing in the cluster database API of Expressway and TelePresence VCS, the first of the issues can be exploited to launch directory traversal attacks and overwrite arbitrary files on the underlying OS, with root privileges.

Affecting the web-based management interface of the two appliances, the second bug can be exploited for arbitrary code execution, Cisco explains in an advisory.

Both vulnerabilities exist because user-supplied command arguments are not sufficiently validated, thus allowing an attacker to authenticate to the system with administrative privileges and then submit crafted input. Release 14.0.5 addresses these issues.

[READ: NSA Informs Cisco of Vulnerability Exposing Nexus Switches to DoS Attacks]

This week, Cisco also released software updates to resolve two high-severity vulnerabilities in Ultra Cloud Core - Subscriber Microservices Infrastructure (SMI) and Identity Services Engine (ISE).

The first of the issues impacts the Common Execution Environment (CEE) ConfD CLI of Ultra Cloud Core SMI and can be exploited by an authenticated, local attacker to access privileged containers as root. The bug is tracked as CVE-2022-20762 (CVSS score of 7.8) and was addressed with the release of Ultra Cloud Core SMI 2020.02.2.47 and 2020.02.7.07.

Impacting the RADIUS feature of ISE, the second bug could be exploited remotely, without authentication, to cause a denial of service (DoS) condition. Tracked as CVE-2022-20756 (CVSS score of 8.6), the flaw exists because certain RADIUS requests are not properly handled. Cisco ISE 2.7P6, 3.0P5, and 3.1P1 contain fixes for this vulnerability.

The tech giant says it is not aware of any of these vulnerabilities being exploited in attacks. However, Cisco customers are advised to update to a patch release as soon as possible.

Related: Cisco Patches Critical Vulnerabilities in Small Business RV Routers

Related: Malicious Emails Can Crash Cisco Email Security Appliances

Related: Cisco Patches Critical Vulnerability in Contact Center Products

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:
Infusion Pumps Impacted by Years-Old Critical Vulnerabilities: Report
BastionZero Raises $6M Seed for Secure Remote Access Tech
Healthcare Company Mon Health Discloses Second Data Breach
Cisco Patches Critical Vulnerabilities in Expressway, TelePresence VCS Products
Microsoft Defender Takes Aim at Mid-Market

Tags:
NEWS & INDUSTRY Vulnerabilities