Cisco Patches High-Severity Security Flaws in IOS XR

By Ionut Arghire on September 10, 2021

Cisco this week released patches for multiple high-severity vulnerabilities in the IOS XR software and warned that attackers could exploit these bugs to reboot devices, elevate privileges, or overwrite and read arbitrary files.

The most severe of these issues is CVE-2021-34720 (CVSS score 8.6), a bug that could be exploited remotely without authentication to exhaust device packet memory, leading to a denial of service (DoS) condition.

The issue was identified in the IP Service Level Agreements (IP SLA) responder and Two-Way Active Measurement Protocol (TWAMP) features of IOS XR and exists because socket creation failures are not handled correctly during the IP SLA and TWAMP processes.

By sending specific IP SLA or TWAMP packets, an attacker could trigger the vulnerability to exhaust the packet memory. This could result in the crash of the IP SLA process or could affect other processes, such as routing protocols.

Cisco also patched a separate issue (CVE-2021-34718, CVSS 8.1) in the SSH Server process of IOS XR that could be exploited by a remote attacker to overwrite and read arbitrary files. Exploitation of this bug requires authentication.

[READ: Microsoft Warns of Information Leak Flaw in Azure Container Instances]

The issue exists because arguments that the user supplies for a specific file transfer method aren't sufficiently validated. Thus, a low-privileged attacker could specify Secure Copy Protocol (SCP) parameters at authentication, which could allow them to elevate privileges and retrieve and upload files on a device.

Two other high severity privilege escalation bugs (CVE-2021-34719 and CVE-2021-34728) were also addressed in IOS XR, along with a denial of service flaw (CVE-2021-34713) affecting ASR 9000 series aggregation services routers that could lead to line card reboots.

Software updates were released to address all of these vulnerabilities and Cisco says it is not aware of any public exploits or malicious attacks targeting them.

Seven other security bugs were addressed in IOS XR software this week, all rated medium severity. Cisco included all of these vulnerabilities in its September 2021 semi-annual bundle of IOS XR Software security advisories.

In a separate advisory on Thursday, the U.S. government's Cybersecurity and Infrastructure Security Agency (CISA) urged organizations to apply the Cisco patches as soon as possible.

"An attacker could exploit some of these vulnerabilities to take control of an affected system. […]CISA encourages users and administrators to review the […] Cisco advisories and apply the necessary updates," CISA said.

Related: Cisco Patches Critical Enterprise NFVIS Vulnerability

Related: Cisco Patches Serious Vulnerabilities in Data Center Products

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Mēris Botnet Flexes Muscles With 22 Million RPS DDoS Attack
Google Introduces Private Compute Services for Android
Cisco Patches High-Severity Security Flaws in IOS XR
HAProxy Vulnerability Leads to HTTP Request Smuggling
GitHub Patches Security Flaws in Core Node.js Dependencies

Tags:

Cyberwarfare Endpoint Security Network Security NEWS & INDUSTRY Application Security Audits Email Security Fraud & Identity Theft Incident Response Compliance Identity & Access Phishing Risk Management Virus & Malware Cloud Security Malware Vulnerabilities Data Protection