# NSA Informs Cisco of Vulnerability Exposing Nexus Switches to DoS Attacks

By Ionut Arghire on February 24, 2022



**Cisco this week announced the availability of patches for four vulnerabilities in its FXOS and NX-OS network operating systems, including one denial of service bug that was reported by the NSA.**

The most severe of the security holes – based on its CVSS score of 8.8 – is CVE-2022-20650, a command injection issue that can be exploited remotely, without authentication to execute arbitrary commands as root.

The bug exists because user supplied data isn't sufficiently validated, thus allowing an attacker to send a crafted HTTP POST request to the NX-API feature on the affected device, to execute commands on the operating system. The NX-API feature, Cisco notes, is disabled by default.

Nexus 3000, 5500, 5600, 6000, and 9000 series switches are affected by this vulnerability if they run an unpatched NX-OS software release and have the NX-API feature enabled.

All of the three remaining vulnerabilities could be exploited to cause denial of service (DoS) conditions.

The flaw reported by the NSA affects the Fabric Services over IP (CFSoIP) feature of NX-OS. Tracked as CVE-2022-20624, this high-severity bug exists because incoming CFSoIP packets aren't sufficiently validated, thus allowing an attacker to send crafted packets to exploit it.

The issue impacts Nexus 3000 and 9000 series switches and UCS 6400 series fabric interconnects, if CFSoIP is enabled (the feature is disabled by default). The NSA hasn't shared additional details about the flaw.

Tracked as CVE-2022-20623, another DoS issue was identified in the rate limiter for Bidirectional Forwarding Detection (BFD) traffic of NX-OS and can be exploited remotely, without authentication to cause BFD traffic to be dropped. Only Nexus 9000 series switches in standalone NX-OS mode are impacted.

The flaw exists because of a logic error in the BFD rate limiter functionality and could be exploited by sending a crafted stream of traffic through the vulnerable device, resulting in dropped IPv4 and IPv6 traffic and leading to a DoS condition.

**[READ: Cisco Patches Critical Vulnerabilities in Small Business RV Routers]**

Cisco also announced the release of an additional fix for CVE-2021-1586, a DoS vulnerability it initially addressed in August 2021, in the Multi-Pod or Multi-Site network configurations for Nexus 9000 series switches in Application Centric Infrastructure (ACI) mode.

The issue exists due to the improper sanitization of TCP traffic sent to a specific port, allowing an attacker to send crafted data.

Cisco encourages customers to apply the latest fixes for their devices, which were released as part of the February 2022 Semiannual FXOS and NX-OS security updates. The company says it is not aware of any of these bugs being exploited in attacks.

**Related:** Malicious Emails Can Crash Cisco Email Security Appliances

**Related:** Cisco Patches Critical Vulnerability in Contact Center Products

**Related:** Cisco Plugs Critical Holes in Catalyst PON Enterprise Switches



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

NSA Informs Cisco of Vulnerability Exposing Nexus Switches to DoS Attacks
Deadbolt Ransomware Targeting Asustor NAS Devices
anecdotes Raises $25 Million for Its Compliance OS Platform
New 'Cyclops Blink' Malware Linked to Russian State Hackers Targets Firewalls
Salesforce Paid Out $12.2 Million in Bug Bounty Rewards to Date



**Tags:**

Network Security NEWS & INDUSTRY Vulnerabilities