Cisco NX-OS Software Image Verification Bypass Vulnerability

Overview

A vulnerability in the bootloader of Cisco NX-OS Software could allow an attacker to bypass image signature verification, allowing for the loading of unverified software. Exploitation requires either physical access to the affected device or administrative credentials on the system.

CVE-2024-20397 (CVSS 5.2) stems from insecure bootloader settings. An attacker can execute specific bootloader commands to bypass image signature verification. Successful exploitation may allow the loading of unauthorized or malicious software.

This vulnerability affects the following Cisco platforms using a vulnerable BIOS version:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Fabric Switches (ACI mode and standalone)
- UCS 6400/6500 Series Fabric Interconnects

Unpatched vulnerabilities can lead to system outages, which may disrupt business operations and cause financial losses. Aspire recommends patching this vulnerability as soon as possible.

Aspire Protects

- **Patch –** Cisco has released patches to address this vulnerability, but no workarounds are available. Please see Cisco's security advisory for patch guidance.
- Only products supporting secure boot technology are affected. Confirm the BIOS version using the show version command.
- Limit physical and administrative access to authorized personnel only.

TTPs to Watch

- **Initial Access**
    - Exploit Public-Facing Application (T1190) – While this scenario primarily requires physical or administrative access, attackers may also use adjacent vulnerabilities to gain a foothold.
- **Privilege Escalation**
    - Abuse Elevation Control Mechanism (T1548.002) – Threat actors could leverage privileged credentials to modify the bootloader settings.

IoCs

There are no known IoCs associated with CVE-2024-20397 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

There are industries that rely on Cisco's high-performance networking equipment, and a vulnerability like this could disrupt operations, expose sensitive data, or impact compliance efforts. Those industries may include:

- Energy and Utilities
- Technology and IT Services
- Healthcare
- Government
- Finance
- Education
- Manufacturing and Supply Chain

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

[Cisco NX-OS Software Image Verification Bypass Vulnerability]