PoC Released for Cisco UCS Secure Boot Bypass Vulnerability Affecting Servers and Security Appliances

Author: *Portia S. Cole – CTI Researcher*

TL;DR

A high-severity vulnerability (CVE-2026-20293, CVSS 7.1) in Cisco UCS servers and UCS-based appliances could allow an attacker to bypass UEFI Secure Boot and execute unauthorized software.

Exploitation requires valid credentials for a Cisco user or administrator account. An unauthenticated attacker would need physical access to the device. Public proof-of-concept code is available, but Cisco has not confirmed exploitation. There are no workarounds, and updates are not yet available for every affected platform.

Overview

There is a vulnerability (CVE-2026-20293, CVSS 7.1) in the Unified Extensible Firmware Interface (UEFI) Shell used by Cisco UCS servers and several UCS-based appliances. UEFI Secure Boot is intended to prevent untrusted software from running when a device starts.

The vulnerability exists because memory-write commands remain available in the UEFI Shell when Secure Boot is enabled. An attacker could select the UEFI Shell during startup and modify memory values used by Secure Boot. This would allow the attacker to bypass validation checks and run unauthorized software in the preboot environment.

CVE-2026-20293 affects devices that have UEFI Secure Boot enabled and use a vulnerable BIOS version. An attacker with valid credentials for a user or administrator account could exploit the vulnerability. An attacker without credentials would need physical access to the device.

Cisco appliances such as Secure Email Gateway and Secure Web Appliance require physical keyboard, video and mouse access, which reduces the likelihood of exploitation.

Affected Products

Cisco UCS and Compute Platforms

- 5000 Series Enterprise Network Compute Systems
- UCS B-Series Blade Servers
- UCS C-Series Rack Servers
- UCS C845A M8 Rack Server

Published on: 9/9/2026

- UCS C880A M8 Rack Server
- UCS C885A M8 Rack Server
- UCS E-Series M3 Servers
- UCS E-Series M6 Servers
- UCS S-Series Storage Servers
- UCS X-Series Modular System
- Unified Edge

UCS-Based Cisco Appliances

- Application Policy Infrastructure Controller Servers
- Cisco Telemetry Broker Appliances
- HyperFlex Edge Nodes
- HyperFlex Nodes
- IEC6400 Edge Compute Appliances
- IOS XRv 9000 M7 Appliances
- Nexus Dashboard Appliances
- Secure Email Gateways
- Secure Email and Web Manager
- Secure Endpoint Private Cloud Appliances
- Secure Firewall Management Center Appliances
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server appliances
- Secure Web Appliances

Cisco has released fixes for several platforms. Updates for some affected products are scheduled for September or October 2026. Cisco is aware of publicly available proof-of-concept code but has not observed exploitation.

Impact on Aspire Customers

Aspire customers may use affected Cisco UCS platforms to host applications and other business systems. The vulnerable hardware is also used in several Cisco security appliances, including Secure Firewall Management Center, Secure Email Gateway, Nexus Dashboard and Secure Network Server appliances.

An attacker who exploits the vulnerability could bypass the device's boot security and execute software that Secure Boot would normally block. This could expose information stored on the affected system or allow unauthorized changes.

The vulnerability cannot be exploited remotely without credentials. Physical access is required when valid Cisco credentials are unavailable.

The Common Vulnerability Scoring System (CVSS) rates vulnerabilities from 0 to 10 based on exploitability and potential impact.

- None (0.0): No severity
- Low (0.1–3.9): Limited impact
- Medium (4.0–6.9): Moderate risk
- High (7.0–8.9): Serious impact
- Critical (9.0–10.0): Severe impact requiring urgent attention

Aspire Protects

- **Patch** – Review Cisco's fixed-release table and install the BIOS, Cisco Integrated Management Controller or Host Upgrade Utility update listed for the affected platform. See Cisco's security advisory for more information.
- Apply the Cisco Secure Firewall Management Center hotfix to affected FMC appliances.
- Follow Cisco's product-specific remediation instructions for UCS-based security and network appliances.
- Track products with pending fixes. Several updates are scheduled for September or October 2026.
- Restrict access to physical and virtual keyboard, video and mouse consoles.
- Review Cisco user and administrator accounts. Remove accounts that are no longer required.

TTPs to Watch

Initial Access

- Valid Accounts [T1078]: Attackers may use compromised Cisco user or administrator credentials to access an affected device.

Defense Evasion

- Pre-OS Boot [T1542]: Attackers may use UEFI Shell memory-write commands to bypass Secure Boot and execute unauthorized software before the operating system loads.

IoCs

There are no known IoCs 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

The vulnerability affects organizations that operate vulnerable Cisco UCS servers or UCS-based appliances with UEFI Secure Boot enabled.

- Public Sector
- Education
- Healthcare
- Finance
- Legal & Professional Services
- Retail
- Manufacturing
- Energy

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 cyber attacks.
- **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's 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.

- **NOC Services Notice**
  - If you are an Aspire NOC customer and are affected by any vulnerability in this notice, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

Cisco UCS and UCS-Based Appliances UEFI Shell Secure Boot Bypass Vulnerability