Cisco Secure Workload Vulnerability Allows Unauthenticated Site Admin Access

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

There is a maximum-severity vulnerability in Cisco Secure Workload (CVE-2026-20223, CVSS 10). The flaw allows an unauthenticated remote attacker to gain Site Admin-level access through crafted API requests.

A successful attack may allow the attacker to access sensitive data and make configuration changes across tenant environments. Cisco stated there is currently no evidence of active exploitation, but there are no workarounds available.

Overview

There is a vulnerability in Cisco Secure Workload (CVE-2026-20223, CVSS 10) that allows an unauthenticated remote attacker to gain Site Admin privileges through crafted requests sent to internal REST API endpoints. Cisco stated the issue is caused by insufficient validation and authentication protections when processing API requests.

Affected Products

- Cisco Secure Workload 3.9 and earlier – Migrate to a fixed version
- Cisco Secure Workload 3.10 – Upgrade to 3.10.8.3
- Cisco Secure Workload 4.0 – Upgrade to 4.0.3.17

If exploited, a threat actor may be able to read sensitive information and make configuration changes across tenant boundaries with Site Admin privileges. The vulnerability impacts Cisco Secure Workload Cluster Software deployed in both SaaS and on-premises environments. Cisco confirmed the vulnerability does not impact the web-based management interface.

There are currently no workarounds available for CVE-2026-20223. Cisco Secure Workload SaaS deployments have already been patched, while on-premises customers must manually update affected systems. There is currently no evidence of exploitation in the wild.

Aspire Protects

- **Patch** - Upgrade Cisco Secure Workload systems to the fixed version. See Cisco's advisory for more information.

- Review Secure Workload logs for unusual API activity or unauthorized configuration changes.
- Restrict access to management and API interfaces to trusted administrative networks only.
- Audit tenant-level configuration changes and administrator activity for signs of misuse.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – A threat actor may send crafted requests to vulnerable Cisco Secure Workload REST API endpoints to gain unauthorized access.

Impact

- Data Manipulation [T1565] – A threat actor with Site Admin access may modify configurations across tenant environments.

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

Cisco Secure Workload is often used in large enterprise and hybrid environments. Organizations using the platform for network segmentation and access control should patch affected systems as soon as possible.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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 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 Secure Workload Unauthorized API Access Vulnerability