CYBER ADVISORY

Friday, May 22, 2026 **CAL-CSIC-202605-A-013**

Critical Cisco Secure Workload Vulnerability

Cisco	Authentication Bypass	API exploitation	Patch Available

The Cybersecurity Integration Center (CSIC) has identified a maximum-severity authentication bypass vulnerability within the internal architecture of the Cisco Secure Workload platform, tracked as CVE-2026-20223 and assigned the *maximum* CVSS 3.1 base score of 10.0[1]. This flaw stems from insufficient validation and lack of authentication checks within the platform's internal REST API endpoints. Successful exploitation allows an unauthenticated remote attacker to bypass security mechanisms by sending a crafted API request, effectively gaining administrative privileges equivalent to the Site Admin role[2]. In summary, the exploitation of this flaw enables remote threat actors to bypass all security checks to gain administrative control over an infrastructure without needing credentials nor a security token.

Cisco Secure Workload is widely used by corporations, hospitals, and government agencies to monitor and manage network traffic to secure sensitive data. Furthermore, Cisco Secure Workload Cluster software is leveraged across both on-premises and cloud-based Software-as-a-Service (SaaS) environments as such, CVE-2026-20223 impacts both device configurations. While the platform's web-based management user interface is unaffected, the vulnerability lies entirely within the internal REST APIs used for backend communication. There are no workarounds available to mitigate this risk. Cisco has already applied updates to automatically remediate its SaaS infrastructure and has released fixed software updates for on-premises deployments. There is currently no confirmed evidence of active exploitation in the wild. However, maximum-severity flaws that grant remote administrative access *rarely* remain unexploited.

Cal-CSIC Analyst Comment: *Given that this type of vulnerability closely follows other highly targeted networking infrastructure campaigns such as the recent zero-day exploitation of Cisco Catalyst SD-WAN controllers, it is highly likely that threat actors will analyze the patch files to reverse-engineer working exploit payloads*[3].

The Cal-CSIC strongly recommends that all organizations managing on-premises instances of Cisco Secure Workload urgently schedule emergency maintenance to apply the published security updates.

Affected administrators running version 3.10 must update to 3.10.8.3, and those on version 4.0 must update to 4.0.3.17. Organizations running legacy versions 3.9 or earlier are entirely unsupported and must prioritize an immediate migration path to a fixed release to prevent full infrastructure compromise.

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NIST; "CVE-2026-20223 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-20223; accessed 21 May 2026
[2] Cisco; "Cisco Secure Workload Unauthorized API Access Vulnerability"; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-pnbsa-g8WEnuy; accessed 21 May 2026
[3] Cisco Talos; "Active exploitation of Cisco Catalyst SD-WAN by UAT-8616"; https://blog.talosintelligence.com/uat-8616-sd-wan/; accessed 21 May 21, 2026