CYBER ADVISORY

Friday, June 5, 2026 **CAL-CSIC-202606-A-003**

Active Exploitation of Cisco Catalyst

Improper Input Validation | Authentication Bypass | Privilege Escalation | Patch Available

The Cybersecurity Integration Center (CSIC) has become aware of a privilege escalation vulnerability in Cisco Catalyst SD-WAN Manager. This vulnerability is tracked as CVE-2026-20245 with a CVSS 3.1 base score of 7.8[1]. The flaw allows an authenticated attacker with network administrator-level access to escalate privileges to root by exploiting improper input validation within the system's CLI (command line interface) functionality. Successful exploitation enables execution of arbitrary commands on the underlying operating system, resulting in full administrative control of the SD-WAN Manager instance and the ability to manipulate SD-WAN fabric configurations.

While this vulnerability does not provide initial access on its own, it poses a significant risk when chained with authentication bypass vulnerabilities such as CVE-2026-20127 or CVE-2026-20182[2], which enables unauthenticated attackers to gain network admin-level access to SD-WAN components. In summary, when either of the vulnerabilities are chained with CVE-2026-20245, a threat actor could move from unauthenticated network access to full control of SD-WAN management infrastructure.

Cisco customers are encouraged to first audit the scripts.log file, located at /var/log/ to for possible indicators of compromise. After which, customers are urged to update to the latest fixed software versions[3]. Cisco states that there are no workarounds available.

Analyst Note: *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 just last month, and that there is already confirmed exploitation - it is highly likely that threat actors will continue to exploit Cisco Catalyst[4].*

The Cal-CSIC strongly recommends that all organizations follow the remediation guidance provided by Cisco.

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] Cisco; "Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability" https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx; accessed 5 June 2026

[2] Rapid7; "CVE-2026-20182: Critical authentication bypass in Cisco Catalyst SD-WAN Controller (FIXED)"; https://www.rapid7.com/blog/post/ve-cve-2026-20182-critical-authentication-bypass-cisco-catalyst-sd-wan-controller-fixed/; accessed 5 June 2026

[3] Cisco; "Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability"; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW; accessed 6 May 2026