CYBER ADVISORY

Thursday, June 18, 2026 **CAL-CSIC-202606-A-012**

Multiple Vulnerabilities Impacting Cisco ISE and Cisco ISE-PIC

Remote Code Execution	Elevation of Privileges	Information Disclosure	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two vulnerabilities impacting Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC). CVE-2026-20181 carries a CVSS 3.1 score of 9.1 and CVE-2026-20190 carries a CVSS 3.1 score of 7.5.[1, 2] The vulnerabilities are not chained or dependent on each other.

CVE-2026-20181 is a Remote Code Execution vulnerability due to insufficient validation of user-supplied input. The vulnerability would allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system of the targeted device. Successful exploitation allows the attacker to obtain user-level access to the underlying operating system to elevate privileges to *root*.[3]

CVE-2026-20190 is an Information Disclosure vulnerability due to improper authorization checks when a resource is accessed. The vulnerability would allow an unauthenticated, remote attacker to view sensitive information on the targeted device by sending crafted traffic to that targeted device. Successful exploitation would allow an attacker to gain access to sensitive information, including hashed credentials that could be used for follow-on attacks.[4]

Cisco has acknowledged these vulnerabilities and has published a security advisory with fixed software releases Cisco ISE and ISE-PIC. Please note that fixed releases for ISE Engines older than ISE 3.2 will not be available due to End-of-Support and upcoming End-of-Support dates established by Cisco. There are no workarounds for these two vulnerabilities. There is no Proof-of-Concept for either of these vulnerabilities, nor is there evidence of them being exploited in the wild or as a zero-day.

The Cal-CSIC recommends following Cisco's remediation guidance as soon as possible. For additional details for both CVE-2026-20181 and CVE-2026-20190, please use these links:

Cisco Security Bulletin:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv

Fixed Software Release Link: https://www.cisco.com/c/en/us/support/security/identity-services-engine/series.html

Affected Product(s) and Version(s) for both CVEs

These Products affect both Cisco ISE and Cisco ISE-PIC regardless of device configuration

Product	Affected ISE Version	Fixed Release Status
Cisco ISE Cisco ISE-PIC	3.5 3.4 3.2	Available
	3.2 3.1	Not Available End of Support Date 30-November 2027
	3.0	Not Available End-of Support 13-July-2025

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] CVEFeed; “CVE-2026-20181”; https://cvefeed.io/vuln/detail/CVE-2026-20181; accessed 18 June 2026
[2] CVEFeed; “CVE-2026-20190”; https://cvefeed.io/vuln/detail/CVE-2026-20190; accessed 18 June 2026
[3] Cisco; “Cisco Identity Services Engine Remote Code Execution and Information Disclosure Vulnerabilities ”; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv; accessed 18 June 2026
[4] Cisco; “Cisco Identity Services Engine Remote Code Execution and Information Disclosure Vulnerabilities ”; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv; accessed 18 June 2026