



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Thursday, September 17, 2026

CAL-CSIC-202609-A-010

Zero-Day Vulnerability Actively Exploited within Cisco Identity Services Engine (ISE) and Cisco ISE-PIC

Unauthorized Access

Zero-Day Vulnerability

Under Active Exploitation

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a zero-day vulnerability actively being exploited within Cisco's Identity Services Engine (ISE) and Cisco's ISE Passive Identity Connector. This vulnerability is due to insufficient authentication control on an API endpoint. CVE-2026-76460 carries the maximum CVSS 3.1 score of 10.0.¹

CVE-2026-76460 is an Incorrect Use of Privileged APIs vulnerability that would enable an attacker to exploit the vulnerability by sending a crafted request to an affected API endpoint. Successful exploitation would allow the attacker to gain unauthorized access to the affected device by bypassing the web-based management interface to obtain command execution with root access.²

Cisco has acknowledged the zero-day vulnerability and have issued patches to address the issue. Workarounds and mitigations are considered temporary solutions. Additionally, Cisco is aware of active exploitation of this vulnerability and have strongly advised that their customers upgrade to an appropriate fixed software release.

The Cal-CSIC recommends following Cisco's remediation guidance and installing their latest patches as soon as possible. It is also important to note that this vulnerability is one of many within Cisco's comprehensive internal security review, and that this particular vulnerability is the only one found to be actively exploited.³

For additional details regarding CVE-2026-76460 or their ISE Hardening release for September 2026, please use these URLs:

Cisco ISE Security Advisory:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>

Cisco ISE Hardening Release 09-2026:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

This vulnerability affects Cisco ISE and Cisco ISE Passive Identity Connector (ISE-PIC), regardless of device configuration.

Affected Products and Fixed Versions

Release	Fixed Version
3.1	3.1 Patch 12
3.2	3.2 Patch 11
3.3	3.3 Patch 12
3.4	3.4 Patch 7
3.5	3.5 Patch 4

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 OpenCVE; "CVE-2026-76460"; <https://app.openCVE.io/cve/CVE-2026-76460>; accessed 17 September 2026

² Cisco; "Cisco Identity Services Engine Authentication Bypass Vulnerability"; <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>; accessed 17 September 17, 2026

³ Cisco; "Cisco Identity Services Engine Hardening Release: September 2026"; <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T>; accessed 17 September 17, 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR