

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

Cisco ISE Authentication Bypass Zero-Day Under Active Exploitation

Date of Publication

September 18, 2026

Admiralty Code

A1

TA Number

TA2026274

Summary

First Seen: September 16, 2026

Affected Products: Cisco Identity Services Engine (ISE), Cisco ISE Passive Identity Connector (ISE-PIC)

Impact: Cisco has confirmed that a critical flaw in its Identity Services Engine (ISE), the platform many organizations rely on to decide who and what is allowed onto their network, is being actively exploited. Tracked as CVE-2026-76460 and carrying the maximum CVSS score of 10.0, the vulnerability lets a remote attacker slip past authentication entirely by sending a specially crafted request to a vulnerable API endpoint. Both Cisco ISE and its companion ISE Passive Identity Connector (ISE-PIC) are affected regardless of how they are configured. Cisco has not named the attackers or shared details of the campaign, but it has warned that a successful exploit can hand an intruder command execution with root privileges; it is essential to patch, as the exploitation is active.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-76460	Cisco Identity Services Engine Incorrect Use of Privileged APIs Vulnerability	Cisco ISE & ISE-PIC			

Vulnerability Details

#1

Cisco has sounded the alarm on a maximum-severity weakness in Identity Services Engine (ISE) that attackers are already abusing in the wild. At its core, CVE-2026-76460 is an authentication bypass. Cisco classifies it under CWE-648 (Incorrect Use of Privileged APIs), and the root cause is straightforward: one of ISE's API endpoints does not properly verify whether the caller is authorized. That single missing control is enough to undo the protection the entire product is built to provide.

#2

Exploiting it is unfortunately simple. A remote attacker only needs network reach to the affected API and can send a crafted request to it, there is no need for valid credentials, no need to trick a user, and no special conditions on the target. That combination is exactly why the flaw earns a perfect 10.0.

#3

The exposure is broad. The bug affects Cisco ISE and ISE-PIC across releases 3.0 through 3.5, regardless of configuration, so a default install is just as vulnerable as a hardened one. Worse, bypassing the login is often only the beginning; Cisco warns that a successful exploit can lead to command execution with root privileges. At that level of access, an intruder effectively owns the appliance and can tamper with or delete the local evidence of what they did.

#4

This is not a theoretical risk. Cisco's PSIRT has confirmed active exploitation in the wild; the company uncovered the issue while resolving a customer support (TAC) case. Cisco has published fixed releases: 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7, and 3.5 Patch 4, and because there is no true workaround, upgrading is the only reliable way to close the door.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-76460	Cisco ISE & ISE-PIC (Releases 3.0 through 3.5, before the first fixed release)	cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*:*:*:*:*:*	CWE-648

Recommendations



Patch Without Delay: Upgrade every affected node to the first fixed release for your train: 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7, or 3.5 Patch 4. Release 3.0 has reached the end of software maintenance and must be migrated to a supported, fixed release. Because the flaw is under active attack and there is no workaround that fully addresses it, patching is the only reliable remediation and should be treated as an emergency change.



Hunt for Signs of Compromise: On every node in the deployment, review the ISE access logs for suspicious or unexpected usernames, and remember this must be done per node in a distributed deployment. Since an attacker with root can wipe or hide local evidence, also cross-check firewall and network logs kept off the device for unusual activity, such as unexpected outbound uploads to external IP addresses or downloads from suspicious hosts. If any sign of malicious activity is found, re-image the affected nodes and restore from a known-good configuration backup.



Apply the Interim Mitigation: Where you cannot patch immediately, restrict who can even reach the device. Use infrastructure access control lists (iACLs) to permit only the required management and control-plane traffic destined for ISE. This does not fix the vulnerability, but it shrinks the attack surface by keeping the vulnerable API out of reach of untrusted networks while you schedule the upgrade.



Treat Exploited Nodes as Fully Compromised: A successful exploit can grant root-level command execution, which means a confirmed hit should be assumed to be a full appliance compromise rather than a contained event. Do not attempt to clean in place, rebuild from trusted media and restore configuration from backup, then rotate any credentials, certificates, or secrets that the node held.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Privilege Escalation	<u>T1068</u> : Exploitation for Privilege Escalation	
Resource Development	<u>T1588</u> : Obtain Capabilities	<u>T1588.006</u> : Vulnerabilities



Patch Link

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



References

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



What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

September 18, 2026 • 07:45 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com