

Alert Bulletin

Bulletin N.: 101

Publication Date: 17/09/2026

Subject: Alert 2026-101 Critical Zero-day in Cisco ISE and ISE-PIC — CVE-2026-76460

Traffic Light Protocol (TLP): White

Affected product(s):

The vulnerability affects **Cisco ISE** and **Cisco ISE PIC**, regardless of device configuration. Cisco has published fixes for the following supported branches:

Product	Affected Branch	Minimum Fixed Version
Cisco Identity Services Engine (ISE)	3.1	3.1 Patch 12
Cisco Identity Services Engine (ISE)	3.2	3.2 Patch 11
Cisco Identity Services Engine (ISE)	3.3	3.3 Patch 12
Cisco Identity Services Engine (ISE)	3.4	3.4 Patch 7
Cisco Identity Services Engine (ISE)	3.5 / 3.5.3	3.5 Patch 4
Cisco ISE Passive Identity Connector (ISE PIC)	Supported vulnerable versions	Apply the equivalent patch for the deployed branch

*Cisco ISE Software Release 3.0 has reached **end of software maintenance**, so it does not have a corrective update for this vulnerability. Teams remaining on that branch should plan an upgrade to a supported release as a priority.

Description

A **critical** authentication bypass vulnerability has been published in Cisco Identity Services Engine (**ISE**) and Cisco ISE Passive Identity Connector (**ISE PIC**), identified as **CVE 2026 76460** with a **CVSS 10.0** score. It allows an unauthenticated remote attacker to send a specially crafted request to an affected API endpoint, bypass authentication on the administration web interface, and obtain unauthorized access to the device.

Cisco confirmed that the vulnerability is being **actively exploited**.

Since ISE typically acts as a central component for network access control, authentication, and identity policies, a compromise can affect identity management, user and device access to the network, and the organization's security posture. It is recommended to update all affected ISE/ISE-PIC nodes with maximum priority and perform a compromise review.

Cisco PSIRT confirmed awareness of active exploitation in real environments, although it has not published details about the responsible actor, the exact attack method, or the affected organizations.

Cisco recommends reviewing the ISE access.log file for suspicious usernames, in particular the dummyuser. In distributed deployment environments, the review must be performed on **each node** of ISE/ISE-PIC.bleepingcomputer+1

Run the following command on each node:

```
admin#show logging application ise-kong/access.log | include dummyuser
```

The presence of entries related to dummyuser in the output should be treated as an **indicator of potential malicious activity** and requires immediate investigation.

Additionally, it is recommended to investigate:

- Unusual logins, API sessions, and administrative changes.
- Accounts, roles, or privileges created or modified outside of maintenance windows.
- Unexpected changes in authentication, authorization, posture policies, endpoint profiles, *network device groups*, or integrations.
- Anomalous outbound network connections from ISE/ISE-PIC nodes.
- Unauthorized processes, services, scheduled tasks, files, or binaries, considering possible root access.
- Unexpected differences between the current configuration and backups/approved configurations.

Solution

Cisco updates for CVE-2026-76460 must be **immediately applied** on all ISE and ISE-PIC nodes. Prioritize administration nodes, *Policy Administration Nodes (PAN)*, nodes exposed or reachable from VPN, user networks, branch offices, third-party environments, and untrusted segments.

Upgrade to the minimum fixed version for each branch: 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7, or 3.5 Patch 4. For unsupported branches, migrate to a supported release that includes the fix.

Below we share helpful links for the upgrade process:

- **Official Cisco ISE Upgrade Guide (Upgrade Journey):**

[Cisco Identity Services Engine Upgrade Journey](#)

This guide centralizes planning, compatibility, backups, node upgrade, and application of *patches* for ISE.

- **Cisco ISE 3.5 Installation and Maintenance Guide:**

- [Cisco ISE Installation Guide, Release 3.5](#)

- Includes requirements, maintenance tasks, and considerations for appliance or virtual machine installations.

- **Upgrade/Patch history verification:**

- [View installation and upgrade history — Cisco ISE](#)

- Cisco indicates using the show version history command from the ISE CLI to review installations, upgrades, uninstalls, and applied *patches*.

- **Official Advisory for CVE 2026 76460:**

- [Cisco PSIRT — Cisco Identity Services Engine Authentication Bypass Vulnerability](#)

- Includes fixed versions, *hardening* instructions, and the required security *patches* to remediate the vulnerability.

Additional information:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
- https://www.cisco.com/c/en/us/td/docs/security/ise/upgrade_guide/b_ise_upgrade_journey.html
- https://www.cisco.com/c/en/us/td/docs/security/ise/3-5/install_guide/b_ise_Installation_Guide_35/g_systemrequirements.html
- https://www.cisco.com/c/en/us/td/docs/security/ise/3-5/install_guide/b_ise_Installation_Guide_35/g_maintenancetasks/t_viewinstallupgradehistory.html