



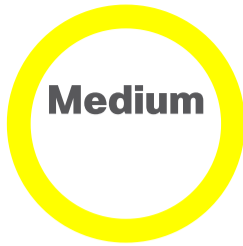
Log in



[Home](#) / [Cisco Security](#) / [Security Advisories](#)

 **Unleash the Power of TAC's Virtual Assistance** ✕
[Activate Cisco In Product Support](#) 

Cisco Identity Services Engine Authenticated Privilege Escalation Vulnerability



Advisory ID:
cisco-sa-ise-cmd-inj-5WSJcYJB

First Published:
2026 April 15 16:00 GMT

Version 1.0: [Final](#)

Workarounds: No workarounds available

Cisco Bug IDs:
[CSCwp98770](#)

CVE-2026-20136

CWE-116

CVSS Score:
[Base 6.0](#) 

[Download CSAF](#)

[Email](#)

^ Summary

A vulnerability in the CLI of Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, local attacker with administrative privileges to perform a command injection attack on the underlying operating system and elevate privileges to *root*.

This vulnerability is due to insufficient validation of user supplied input. An attacker could exploit this vulnerability by providing crafted input to a specific CLI command. A successful exploit could allow the attacker to elevate their privileges to *root* on the underlying operating system.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-5WSJcYJB>

^ Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected Cisco ISE and ISE-PIC, regardless of device configuration.

For information about which Cisco software releases were vulnerable at the time of publication, see the [Fixed Software](#) section of this advisory. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

Products Confirmed Not Vulnerable

Only products listed in the [Vulnerable Products](#) section of this advisory are known to be affected by this vulnerability.

^ Workarounds

There are no workarounds that address this vulnerability.

^ Fixed Software

Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Fixed Releases

At the time of publication, the release information in the following table was accurate. See the Details section in the bug ID at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

Cisco ISE or ISE-PIC Release	First Fixed Release
3.3 and earlier	3.3 Patch 11 (Apr 2026)
3.4	3.4 Patch 6 (Apr 2026)
3.5 ¹	3.5 Patch 3

1. Cisco ISE-PIC has reached the end-of-sale date. Release 3.4 is the last supported release.

For instructions on upgrading a device, see the Upgrade Guides on the [Cisco Identity Service Engine](#) support page.

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

^ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

^ Source

Cisco would like to thank Kentaro Kawane of GMO Cybersecurity by Ierae for reporting this vulnerability.

^ URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-5WSJcYJB>

^ Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2026-APR-15

^ Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT

The [Cisco Support and Downloads](#) page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the [Cisco Technical Assistance Center \(TAC\)](#). Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

When [considering software upgrades](#), customers are advised to regularly consult [the advisories](#) for the relevant Cisco products to determine exposure and a complete upgrade solution. In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the [Cisco Technical Assistance Center \(TAC\)](#) or their contracted maintenance providers.

LEGAL DISCLAIMER DETAILS

CISCO DOES NOT MAKE ANY EXPRESS OR IMPLIED GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CISCO DOES NOT GUARANTEE THE ACCURACY OR COMPLETENESS OF THIS INFORMATION. THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the [Cisco Security Advisories](#) page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the [Cisco Security Vulnerability Policy](#) for more information.

▶ [Cisco Security Vulnerability Policy](#)

▶ [Subscribe to Cisco Security Notifications](#)

▶ [Related to This Advisory](#)

Quick Links

[About Cisco](#)

[Contact Us](#)

[Careers](#)

[Connect with a partner](#)

Resources and Legal

[Feedback](#)

[Help](#)

[Terms & Conditions](#)

[Privacy](#)

[Cookies / Do not sell or share my personal data](#)

[Accessibility](#)

[Trademarks](#)

[Supply Chain Transparency](#)

[Newsroom](#)

[Sitemap](#)



© 2026 Cisco Systems, Inc.

 **Unleash the Power of TAC's Virtual Assistance** ×
[Activate Cisco In Product Support](#) ▶