Cisco Security Advisory

Cisco Identity Services Engine Remote Code Execution and Path Traversal Vulnerabilities

Advisory ID:
cisco-sa-ise-rce-traversal-8bYndVrZ

First Published:
2026 April 15 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCws52717 , CSCws52738

CVE-2026-20147

CVE-2026-20148

CWE-22

CWE-77

CVSS Score:
Base 9.9

Download CSAF

Email

Summary

Multiple vulnerabilities in Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, remote attacker to achieve remote code execution or conduct path traversal attacks on an affected device. To exploit these vulnerabilities, the attacker must have valid administrative credentials.

For more information about these vulnerabilities, see the Details section of this advisory.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ

Affected Products

Vulnerable Products

These vulnerabilities affect Cisco ISE and Cisco ISE-PIC, regardless of device configuration.

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by these vulnerabilities.

Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerabilities.

Details about the vulnerabilities are as follows:

CVE-2026-20147: Cisco ISE Remote Code Execution Vulnerability

A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to *root*. In single-node ISE deployments, successful exploitation of this vulnerability could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In th cated would be unable to access the network until the node is restored.

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

Bug ID(s): CSCws52738
CVE ID: CVE-2026-20147
Security Impact Rating (SIR): Critical
CVSS Base Score: 9.9
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE-2026-20148: Cisco ISE Path Traversal Vulnerability

A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to perform path traversal attacks on the underlying operating system and read arbitrary files. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system.

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

Bug ID(s): CSCws52717
CVE ID: CVE-2026-20148
Security Impact Rating (SIR): Medium
CVSS Base Score: 4.9
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

Workarounds

There are no workarounds that address these vulnerabilities.

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 these vulnerabilities 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

In the following table, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerabilities that are described in this advisory and the first release that includes the fix for these vulnerabilities. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

Cisco ISE or ISE-PIC Release	First Fixed Release
Earlier than 3.1	Migrate to a fixed release.
3.1	3.1 Patch 11 (Apr 2026)
3.2	3.2 Patch 10 (Apr 2026)
3.3	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 vulnerabilities that are described in this advisory.

Source

Cisco would like to thank Jonathan Lein of TrendAI Research for reporting these vulnerabilities.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/

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