An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609180207

NCSC Advisory

Critical Vulnerability exists in Cisco ISE Passive Identity Connector and Cisco Identity Services Engine

CVE-2026-76460

18 September 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-76460

Published: 2026-09-16

Vendor: Cisco

Product: Cisco ISE Passive Identity Connector, Cisco Identity Services Engine Software

CVSS Score[1]: 10

Products Affected

Product	Version
Cisco Identity Services Engine Software &Cisco ISE Passive Identity Connector	< 3.1 Patch 12
Cisco Identity Services Engine Software &Cisco ISE Passive Identity Connector	< 3.2 Patch 11
Cisco Identity Services Engine Software &Cisco ISE Passive Identity Connector	< 3.3 Patch 12
Cisco Identity Services Engine Software &Cisco ISE Passive Identity Connector	< 3.4 Patch 7
Cisco Identity Services Engine Software &Cisco ISE Passive Identity Connector	< 3.5 Patch 4

Impact

A vulnerability in an API of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to bypass authentication.

This vulnerability is due to insufficient authentication control on an API endpoint. An attacker could exploit this vulnerability by sending a crafted request to an affected API endpoint. A successful exploit could allow the attacker to gain unauthorized access to the affected device by bypassing the web-based management interface.

[1] https://www.first.org/cvss/

Common Weakness Enumeration (CWE)[2]: CWE-648: Incorrect Use of Privileged APIs

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- https://nvd.nist.gov/vuln/detail/CVE-2026-76460
- https://www.cve.org/CVERecord?id=CVE-2026-76460
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-76460

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog