VULNERABILITY BULLETINS

Cisco Patches Identity Services Engine (ISE) Security Flaw (CVE-2026-20029)

TLP:WHITE

Jan 08, 2026

On January 7, 2026, Cisco released security updates to address a medium-severity vulnerability, tracked as CVE-2026-20029, affecting its Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC) network access control solutions.

This flaw enables an authenticated, remote attacker with administrative privileges to access sensitive files from the underlying operating system that should be restricted. Although there is no evidence of active exploitation, a proof-of-concept (PoC) exploit is publicly available, which significantly increases the risk of potential abuse.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their level of risk to this vulnerability.

Analysis

The vulnerability, identified as CVE-2026-20029 (CVSS 4.9), is an XML external entity (XXE) processing flaw located within the

licensing features of the Cisco ISE web-based management interface. The issue arises from the improper parsing of XML documents processed by the application. An attacker can exploit this vulnerability by uploading a maliciously crafted XML file to the management console, which triggers the server to process external entity references that resolve to files on the local filesystem.

Successful exploitation of this flaw allows a threat actor to perform an unauthorized read of arbitrary files from the underlying operating system. This could include sensitive configuration files, system data, and other information that is intended to be inaccessible even to legitimate administrative users. Such data exfiltration can serve as a precursor to more advanced attacks, providing the information necessary for further privilege escalation or lateral movement within the network.

This vulnerability affects both Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) across multiple release branches. Specifically, all releases prior to 3.2 are affected and require migration to a fixed release. Additionally, the 3.2, 3.3, and 3.4 release lines are vulnerable if they are running a version prior to the first fixed release. Cisco confirmed that this vulnerability affects these products regardless of their specific device configuration.

According to the Cisco Product Security Incident Response Team (PSIRT), there is currently no evidence of active exploitation in the wild. However, the PSIRT has issued a warning that proof-of-concept (PoC) exploit code is publicly available. The existence of public exploit code lowers the barrier for motivated actors to weaponize the flaw, particularly since the attacker only needs valid administrative credentials, which could be obtained through credential harvesting or other separate compromises to carry out the attack.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

1. Apply the available security updates:
    - Cisco ISE/ISE-PIC 3.2: Upgrade to 3.2 Patch 8 or later.
    - Cisco ISE/ISE-PIC 3.3: Upgrade to 3.3 Patch 8 or later.
    - Cisco ISE/ISE-PIC 3.4: Upgrade to 3.4 Patch 4 or later.
    - Versions earlier than 3.2: Migrate to a supported
2. Monitor for unusual administrative file uploads or suspicious activity within the web-based management interface.
3. Ensure that administrative access to the ISE management interface is restricted to trusted internal networks
4. Use multi-factor authentication (MFA) to mitigate the risk of attackers using stolen credentials to exploit this flaw.
5. Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	nist, hhs, cisco, thehackernews, bleepingcomputer

Alert ID 9a7e5f43

View Alert

Share Feedback

was this helpful? |

Tags CVE-2026-20029, Cisco ISE Passive Identity Connector, Cisco ISE-PIC, Cisco ISE, Cisco Identity Services Engine (ISE), Cisco

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**