

CVE-2025-20281

Cisco Identity Services Engine Injection Vulnerability

Exigent

CISA KEV since Jul 28, 2025

Actively exploited

A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit this vulnerability. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to obtain root privileges on an affected device.

EVRS 88/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.976 99.9th percentile · FIRST	CISA DEADLINE Aug 18, 2025 KEV since 2025 · listed over a year
--	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.976 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
identity services engine	3.3.0 3.4.0	no fixed version listed	NVD
identity services engine passive identity connector	3.3.0 3.4.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-rc4f-42xm-hvjw

Additional guidance sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd26nJ6

NVD nvd.nist.gov/vuln/detail/CVE-2025-20281

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-19167

Current data evulnable.com/vulnerability-management/cve/CVE-2025-20281

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.