

CVE-2021-44529

Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection Vulnerability

Exigent
CISA KEV since Mar 25, 2024
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

A code injection vulnerability in the Ivanti EPM Cloud Services Appliance (CSA) allows an unauthenticated user to execute arbitrary code with limited permissions (nobody).

EVRS 93 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.991 99.93rd percentile · FIRST	CISA DEADLINE Apr 15, 2024 KEV since 2024 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.991 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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 or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
endpoint manager cloud services appliance	≤ 4.5 4.6	after 4.5	NVD

Sources

Vendor guidance	forums.ivanti.com/s/article/SA-2021-12-02	forums.ivanti.com	forums.ivanti.com/s/article/SA-2021-12-02?language=en_US
NVD	nvd.nist.gov/vuln/detail/CVE-2021-44529	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-31360	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-44529

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