

CVE-2019-11510

Ivanti Pulse Connect Secure Arbitrary File Read Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.

EVRS

94/100

Immediate priority

CVSS V3.1

10.0

Critical · NVD

EPSS

0.999

99.99th percentile · FIRST

CISA DEADLINE

May 3, 2022

KEV since 2021 · 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	0.999 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 updates per vendor instructions. **CISA note:** Reference CISA's ED 21-03 (<https://www.cisa.gov/news-events/directives/ed-21-03-mitigate-pulse-connect-secure-product-vulnerabilities>) for further guidance and requirements. Note: The due date for addressing this vulnerability aligns with the requirements outlined in ED 21-03. <https://nvd.nist.gov/vuln/detail/CVE-2019-11510>

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connect secure	8.2 8.3 9.0	no fixed version listed	NVD

Sources

Vendor guidance	kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/nvd.nist.gov/vuln/detail/CVE-2019-11510	Additional guidance	kb.pulsesecure.net/?atype=sa
NVD		CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-3183	Current data	evulnable.com/vulnerability-management/cve/CVE-2019-11510

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