

CVE-2021-22899

Ivanti Pulse Connect Secure Command Injection Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

A command injection vulnerability exists in Pulse Connect Secure before 9.1R11.4 allows a remote authenticated attacker to perform remote code execution via Windows Resource Profiles Feature

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.229 97.7th 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.229 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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-2021-22899>
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connect secure	9.0 9.1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-3v8c-432m-393w

Additional guidance kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/?kA23Z000000boUWSAY

NVD nvd.nist.gov/vuln/detail/CVE-2021-22899

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-10031

Current data evulnable.com/vulnerability-management/cve/CVE-2021-22899

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