

CVE-2019-11539

Ivanti Pulse Connect Secure and Policy Secure Command Injection Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, the admin web interface allows an authenticated attacker to inject and execute commands.

EVRS 90 /100 Immediate priority	CVSS V3.1 7.2 High · NVD	EPSS 0.985 99.92nd 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	0.985 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connect secure	8.1	no fixed version listed	NVD
	8.2		
	8.3		
	9.0		
policy secure	9.0	no fixed version listed	NVD



pulse policy secure	5.1r1.0	no fixed version listed	NVD
	5.1r1.1		
	5.1r2.0		
	5.1r2.1		
	5.1r3.0		
	5.1r3.2		
	5.1r4.0		
	5.1r5.0		
	5.1r6.0		
	5.1r7.0		
	5.1r8.0		
	5.1r9.0		
	5.1r9.1		
	5.1r10.0		
	5.1r11.0		
	5.1r11.1		
	5.1r12.0		
	5.1r12.1		
	5.1r13.0		
	5.1r14.0		
	5.2r1.0		
	5.2r2.0		
	5.2r3.0		
	5.2r3.2		
	5.2r4.0		
	5.2r5.0		
	5.2r6.0		
	5.2r7.0		
	5.2r7.1		
	5.2r8.0		
	5.2r9.0		
	5.2r9.1		
	5.2r10.0		
	5.2r11.0		
	5.2rx		
	5.3r1.0		
	5.3r1.1		
	5.3r2.0		
	5.3r3.0		
	5.3r3.1		
	5.3r4.0		
	5.3r4.1		
	5.3r5.0		
	5.3r5.1		
	5.3r5.2		
	5.3r6.0		
	5.3r7.0		
	5.3r8.0		
	5.3r8.1		
	5.3r8.2		
	5.3r9.0		
	5.3r10.		
	5.3r11.0		
	5.3r12.0		
	5.3rx		
	5.4r1		
	5.4r2		
	5.4r2.1		
	5.4r3		
	5.4r4		
	5.4r5		
	5.4r5.2		
	5.4r6		



PACKAGE	AFFECTED	FIXED IN	SOURCE
	5.4r6.1		
	5.4r7		
	5.4rx		

Sources

Vendor guidance github.com/advisories/GHSA-mchx-p635-vpq8

Additional guidance kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

NVD nvd.nist.gov/vuln/detail/CVE-2019-11539

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-3210

Current data evulnable.com/vulnerability-management/cve/CVE-2019-11539

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