An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2504040119

NCSC Advisory

Critical Vulnerabilities in Ivanti: ZTA Gateways, Connect Secure, and Policy Secure

CVE-2025-22457

4th, April 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2025-22457

Published: 2025-04-03

Vendor: Ivanti

Product: Neurons for ZTA Gateways, Connect Secure, Pulse Connect Secure, Policy Secure

CVSS Score[1]: 9.0

Products Affected

Product Name	Affected Version	Resolved Version
Ivanti Connect Secure	22.7R2.5 and prior	22.7R2.6 (released February 2025)
Pulse Connect Secure (EoS)	9.1R18.9 and prior	22.7R2.6
Ivanti Policy Secure	22.7R1.3 and prior	22.7R1.4
ZTA Gateways	22.8R2 and prior	22.8R2.2

Impact

A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6, Ivanti Policy Secure before version 22.7R1.4, and Ivanti ZTA Gateways before version 22.8R2.2 allows a remote unauthenticated attacker to achieve remote code execution.

Ivanti are aware of a limited number of customers whose Ivanti Connect Secure (22.7R2.5 or earlier) and **End-of-Support** Pulse Connect Secure 9.1x appliances have been exploited at the time of disclosure.

Pulse Connect Secure 9.1x reached End-of-Support on December 31, 2024, and no longer receives code support or changes.

Common Weakness Enumeration (CWE)[2]: CWE-121: CWE-121 Stack-based Buffer Overflow

Known Exploited Vulnerability (KEV) catalog[3]: No

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Ivanti.

- https://nvd.nist.gov/vuln/detail/CVE-2025-22457
- https://www.cve.org/CVERecord?id=CVE-2025-22457
- https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457