An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2501080153

NCSC Advisory

Critical Vulnerabilities in Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-0282, CVE-2025-0283)

9th January 2025

STATUS: TLP:CLEAR

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Description

CVE ID: CVE-2025-0282

Published: 2025-01-08T16:55:55

Vendor: Ivanti

Product: Ivanti Connect Secure, Ivanti Policy Secure, Ivanti Neurons for ZTA gateways

CVSS3.0 Score[1]: 9.0

Summary: A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote, unauthenticated attacker to achieve remote code execution.

CVE ID: CVE-2025-0283

Published: 2025-01-08T16:55:55

Vendor: Ivanti

Product: Ivanti Connect Secure, Ivanti Policy Secure, Ivanti Neurons for ZTA gateways

CVSS3.0 Score: 7.0

Summary: A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local, authenticated attacker to escalate their privileges.

Products Affected

CVE-2025-0282

- Ivanti Connect Secure
  - 22.7R2 through 22.7R2.4
- Ivanti Policy Secure
  - 22.7R1 through 22.7R1.2
- Ivanti Neurons for ZTA gateways
  - 22.7R2 through 22.7R2.3

[1] https://www.first.org/cvss/v3.0/specification-document

CVE-2025-0283

- Ivanti Connect Secure
  - 22.7R2.4 and prior, 9.1R18.9 and prior
- Ivanti Policy Secure
  - 22.7R1.2 and prior
- Ivanti Neurons for ZTA gateways
  - 22.7R2.3 and prior

Impact

CVE-2025-0282

Allows a remote, unauthenticated attacker to achieve remote code execution.

- **Common Weakness Enumeration (CWE):** CWE-121[2]
- **Known Exploited Vulnerability (KEV) catalog[3]**: Not Known
- **Used by Ransomware Operators**: Not Known

CVE-2025-0283

Allows a local, authenticated attacker to escalate their privileges.

- **Common Weakness Enumeration (CWE):** CWE-121
- **Known Exploited Vulnerability (KEV) catalog**: Not Known
- **Used by Ransomware Operators**: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Ivanti as soon as possible. More details can be found here: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

Please note: Ivanti are aware of active exploitation of CVE-2025-0282 affecting Ivanti Connect Secure.

Exploitation of CVE-2025-0282 may be identified by the Integrity Checker Tool (ICT). According to Ivanti, the latest ICT version, ICT-V22725, is only designed to operate with version 22.7R2.5, and above, ICS releases.

Ivanti have provided the below potential solutions:

[2] https://cwe.mitre.org/data/definitions/121.html
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Ivanti Connect Secure

- Clean internal and external ICT scan: upgrade to Ivanti Connect Secure 22.7R2.5 and continue to closely monitor your internal and external ICT in conjunction with other security tools. Factory reset (https://forums.ivanti.com/s/article/Recovery-Steps) on appliances with a clean ICT scan is recommended before putting 22.7R2.5 in production out of an abundance of caution.
- ICT result shows signs of compromise: perform a factory reset on the appliance to ensure any malware is removed, put the appliance back into production using version 22.7R2.5. Continue to closely monitor your internal and external ICT in conjunction with other security tools.

Ivanti Policy Secure

According to Ivanti, this solution is not intended to be internet facing, which makes the risk of exploitation significantly lower. The fix for Ivanti Policy Secure is planned for release on January 21, 2025, and will be available in the standard download portal. Customers should always ensure that their IPS appliance is configured according to Ivanti recommendations and not expose it to the internet. They are not aware of these CVEs being exploited in Ivanti Policy Secure.

Ivanti Neurons for ZTA Gateways

According to Ivanti, the Ivanti Neurons ZTA gateways cannot be exploited when in production. If a gateway for this solution is generated and left unconnected to a ZTA controller, then there is a risk of exploitation on the generated gateway. The fix is planned for release on January 21, 2025. They are not aware of these CVEs being exploited in ZTA Gateways.

Further Info:

- CISA Mitigation Instructions for CVE-2025-0282: https://www.cisa.gov/cisa-mitigation-instructions-cve-2025-0282
- Mandiant report: https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/