CERT-EU

Security Advisory 2025-001

Critical Vulnerabilities in Ivanti Products

2025-01-10 — v1.2

TLP:CLEAR

History:

- *09/01/2025 — v1.0 – Initial publication*
- *09/01/2025 — v1.1 – Fix an issue in affected products, and add information about EOL versions*
- *10/01/2025 — v1.2 – Updating the summary about the exploitation of CVE-2025-0282*

Summary

On January 8, 2025, Ivanti announced the release of two critical vulnerabilities affecting their products Ivanti Connect Secure and Ivanti Policy Secure and Ivanti Neurons for ZTA gateways [1]. These vulnerabilities could lead to remote code execution and privilege escalation.

[New] Ivanti's security advisory indicates that **CVE-2025-0282** was being exploited on a limited number of Ivanti Connect Secure appliances at the time of disclosure [1].

It is strongly recommended updating affected devices as soon as possible.

Technical Details

The vulnerability **CVE-2025-0282**, with a CVSS score of 9.0, is stack-based buffer overflow flow allowing a remote unauthenticated attacker to achieve remote code execution.

The vulnerability **CVE-2025-0283**, with a CVSS score of 7.0, is a stack-based buffer overflow allowing a local authenticated attacker to escalate its privileges.

Affected Products

The vulnerability CVE-2025-0282 affects:

- Ivanti Connect Secure 22.7R2 through 22.7R2.4 (patch available)
- Ivanti Policy Secure 22.7R1 through 22.7R1.2 (patch not available)
- Ivanti Neurons for ZTA gateways 22.7R2 through 22.7R2.3 (patch not available)

The vulnerability CVE-2025-0283 affects:

- Ivanti Connect Secure 22.7R2.4 and prior, 9.1R18.9 and prior (patch available)
- Ivanti Policy Secure 22.7R1.2 and prior (patch not available)
- Ivanti Neurons for ZTA gateways 22.7R2.3 and prior (patch not available)

Note: The Ivanti Connect Secure version 9.x reached End of Life on December 31, 2024, and will not be receiving a patch for CVE-2025-0283.

Recommendations

It is strongly recommended checking affected devices for indicators of compromise, **running the external and internal Integrity Checker Tool (ICT)**. When no sign of compromise is being observed, it is strongly recommended updating affected products when possible. When suspicious activities are observed, it is recommended starting a forensic investigation.

Ensure that products that are not supposed to be Internet facing are effectively not (i.e., Ivanti Policy Secure).

Detection

To identify potential compromises, we recommend running both an external and internal ICT scan on affected devices. For guidance on interpreting the results, refer to Mandiant's blog, which provides examples of successful and unsuccessful scans. If you detect any suspicious activity, contact Ivanti Support.

In addition, we recommend to search in the logs for:

- HTTP requests matching the following patterns: `/dana-cached/hc/hc_launcher.` likely to determine the version prior to attempting exploitation [2].
- Suspicious gaps in logging activity, which could indicate an attacker's attempt to cover their tracks [2].

References

[1] https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

[2] https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day?e=48754805