Security Advisory 2025-016

Critical Vulnerability in Ivanti Products

2025-04-04 — v1.0

TLP:CLEAR

History:

- *04/04/2025 — v1.0 – Initial publication*

Summary

On April 4, 2025, Ivanti released a security advisory regarding a critical vulnerability affecting their products. The vulnerability is known to be exploited in the wild. The vulnerability has been fixed in the February 2025 release and was initially identified as a product bug.

CERT-EU recommends upgrading to a supported and fixed version of Ivanti products as soon as possible. CERT-EU also recommends reviewing forensic evidence to detect any signs of exploitation.

Technical Details

The vulnerability **CVE-2025-22457**, with a CVSS score of 9.0, is a stack-based buffer overflow vulnerability. When exploited, it allows for unauthenticated remote code execution on affected devices.

Affected Products

The vulnerability affects the following products and versions:

- Ivanti Connect Secure version 22.7R2.5 and prior
- Ivanti Connect Secure version 9.1R18.9 and prior (this product is End of Life since December 31, 2024)
- Ivanti Policy Secure version 22.7R1.3 and prior
- ZTA Gateways version 22.8R2 and prior

Recommendations

CERT-EU recommends upgrading to a supported and fixed version of Ivanti products as soon as possible. CERT-EU also recommends reviewing forensic evidence to detect any signs of exploitation.

Mitigation

When it is not possible to update immediately, CERT-EU recommends restricting access to vulnerable systems to only trusted sources.

References

[1] https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US