Security Advisory 2022-074

DoS Vulnerabilities in Pulse Secure Products

October 27, 2022 — v1.0

TLP:CLEAR

History:

- *27/10/2022 — v1.0 – Initial publication*

Summary

On October 13, 2022, Ivanti released an advisory regarding two vulnerabilities affecting Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), and Ivanti Neurons for Zero-Trust Gateway that could lead to DoS conditions if exploited [1]. It is recommended to upgrade to the latest version of these products.

Technical Details

Ivanti did not release much technical details about the vulnerabilities, identified by `CVE-2022-35254`, and `CVE-2022-35258`, with CVSS scores of 7.5 out of 10. Nevertheless, the company specified that the vulnerabilities could lead to Denial-of-Service (DoS) conditions if exploited. Based on the CVSS scores, we can guess that the vulnerabilities could be exploited remotely and fairly easily.

Affected Products

CVE-2022-35254 and **CVE-2022-35258** affect:

- Ivanti Policy Secure 9.1R16, 22.2R1 and below
- Ivanti Neurons for Zero-Trust Gateway 22.2R1 and below
- Ivanti Connect Secure 9.1R16.1, 22.2R1 and below

The Ivanti Neurons for Secure Access was affected by both vulnerabilities. Ivanti upgraded the hosted controller and completed the upgrade on October 9, 2022. There is no action for customers to take regarding the Ivanti Neurons for Secure Access Controller.

Recommendations

CERT-EU recommends updating the affected systems to the latest version.

References

[1] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA45520/?kA23Z000000GH5OSAW