Security Advisory 2024-119

Critical Vulnerability in Ivanti Products

2024-12-11 — v1.0

TLP:CLEAR

History:

- *11/12/2024 — v1.0 – Initial publication*

Summary

On December 10, 2024, Ivanti has released critical security updates addressing multiple vulnerabilities in its Cloud Services Appliance (CSA) and Connect Secure products. These flaws could allow attackers to escalate privileges or execute arbitrary code [1,2].

Technical Details

The vulnerability **CVE-2024-11639**, with a CVSS score of 10.0, is an authentication bypass in the CSA admin web console permitting remote unauthenticated attackers to gain administrative access.

The vulnerability **CVE-2024-11772**, with a CVSS score of 9.1, is a command injection in the CSA admin web console allowing remote authenticated attackers with admin privileges to achieve remote code execution.

The vulnerability **CVE-2024-11773**, with a CVSS score of 9.1, is an SQL injection in the CSA admin web console enabling remote authenticated attackers with admin privileges to execute arbitrary SQL statements.

The vulnerability **CVE-2024-11633**, with a CVSS score of 9.1, is an argument injection in Connect Secure that allows remote authenticated attackers with admin privileges to achieve remote code execution.

The vulnerability **CVE-2024-11634**, with a CVSS score of 9.1, is a command injection in Connect Secure and Policy Secure permitting remote authenticated attackers with admin privileges to achieve remote code execution.

The vulnerability **CVE-2024-8540**, with a CVSS score of 8.8, is an insecure permissions issue in Sentry allowing local authenticated attackers to modify sensitive application components.

Affected Products

The following product versions are affected:

- **Ivanti Cloud Services Appliance (CSA)**: Versions prior to 5.0.3;
- **Ivanti Connect Secure**: Versions prior to 22.7R2.4;
- **Ivanti Policy Secure**: Versions prior to 22.7R1.2;
- **Ivanti Sentry**: Versions prior to 9.20.2, 10.0.2, and 10.1.0.

Recommendations

To mitigate these vulnerabilities, CERT-EU strongly recommends to upgrade to the latest versions where the vulnerabilities have been addressed.

References

[1] https://www.ivanti.com/blog/december-security-update

[2] https://thehackernews.com/2024/12/ivanti-issues-critical-security-updates.html