CERT-EU

Security Advisory 2024-030

Critical Vulnerabilities in Ivanti Products

March 21, 2024 — v1.0

TLP:CLEAR

History:

- *21/03/2024 — v1.0 – Initial publication*

Summary

On March 20, 2024, Ivanti released fixes for two critical vulnerabilities affecting Ivanti Standalone Sentry and Ivanti Neurons for ITSM. According to Ivanti, there is no evidence of these vulnerabilities being exploited in the wild.

It is recommended upgrading affected software as soon as possible.

Technical Details

The vulnerability `CVE-2023-41724`, with a CVSS score of 9.6, affects Ivanti Standalone Sentry and could allow an unauthenticated attacker within the same physical or logical network to execute arbitrary commands on the underlying operating system of the appliance. [1]

The vulnerability `CVE-2023-46808`, with a CVSS score of 9.9, affects Ivanti Neurons for ITSM and could enable an authenticated remote user to perform file writes in sensitive directories which may allow execution of commands in the context of web application's user. [2]

Affected Products

The vulnerability `CVE-2023-41724` impacts all supported versions of Ivanti Standalone Sentry (9.17.0, 9.18.0, and 9.19.0). Older versions are also at risk.

The vulnerability `CVE-2023-46808` impacts all supported versions of Ivanti Neurons for ITSM (2023.3, 2023.2 and 2023.1). Unsupported versions are also at risk.

Recommendations

CERT-EU strongly recommends updating affected software to the latest versions by following the instructions given by the vendor [1,2].

References

[1] https://forums.ivanti.com/s/article/CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry?language=en_US

[2] https://forums.ivanti.com/s/article/SA-CVE-2023-46808-Authenticated-Remote-File-Write-for-Ivanti-Neurons-for-ITSM?language=en_US