March 20, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Ivanti published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following:

- Ivanti Neurons for ITSM (2023.3, 2023.2 and 2023.1) – all versions
- Ivanti Standalone Sentry – versions 9.17.0, 9.18.0, 9.19.0 and prior

Technical Details

An authenticated remote user can perform file writes to ITSM server. Successful exploitation can be used to write files to sensitive directories which may allow attackers execution of commands in the context of web application's user.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-46808 CVE-2023-41724
- Ivanti Security Advisory - CVE-2023-46808 (Authenticated Remote File Write) for Ivanti Neurons for ITSM
- Ivanti Security Advisory - CVE-2023-41724 (Remote Code Execution) for Ivanti Standalone Sentry
- Ivanti Security Advisories