December 20, 2023

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Ivanti published a security advisory to address critical vulnerabilities in the following product:

- Ivanti Avalanche – versions prior to 6.4.2

Technical Details

An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result in a Denial of Service (DoS) or code execution.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2023-41727, CVE-2023-46216, CVE-2023-46217, CVE-2023-46220, CVE-2023-46221, CVE-2023-46222, CVE-2023-46223, CVE-2023-46224, CVE-2023-46225, CVE-2023-46257, CVE-2023-46258, CVE-2023-46259, CVE-2023-46260, CVE-2023-46261, CVE-2023-46262, CVE-2023-46266, CVE-2023-46263, CVE-2021-22962, CVE-2023-46264, CVE-2023-46265, CVE-2023-46803
- Ivanti Security Advisory - Avalanche 6.4.2
- Ivanti Security Advisories