

Overall Rating - Critical



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

Summary

The Vulnerability and Risk Management (VRM) Team is aware of multiple vulnerabilities disclosed in Ivanti Avalanche below version 6.4.1.

Technical Details

- An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. Fixed in version 6.4.1. CVE-2023-32566
- Ivanti Avalanche decodeToMap XML External Entity Processing. Fixed in version 6.4.1. CVE-2023-32567

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 as soon as possible.

Please notify [VRM](#) with any questions or concerns you may have.

References

- [CVE-2023-32566](#), [CVE-2023-32567](#)
- https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US