April 19, 2024

**Overall rating: Critical**

BRITISH COLUMBIA

**This is a technical bulletin intended for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Ivanti Avalanche ecurity vulnerabilities. The vulnerability affects Avalanche prior to 6.4.3.

## Technical Details

Avalanche 6.4.3 has addressed some new security hardening and vulnerabilities in our Q1 2024 release. Ivanti is not aware of any exploitation of these vulnerabilities at the time of disclosure.

It is highly recommended to download the Avalanche installer and update to the latest Avalanche 6.4.3. The installation will apply a fix for each CVE listed in the references below. These vulnerabilities affect older versions of Avalanche.

**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 this risk.

## 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-2024-22061, CVE-2024-23526, CVE-2024-23527, CVE-2024-23528, CVE-2024-23529, CVE-2024-23530, CVE-2024-23531, CVE-2024-23532, CVE-2024-23533, CVE-2024-23534, CVE-2024-23535, CVE-2024-24991, CVE-2024-24992, CVE-2024-24993, CVE-2024-24994, CVE-2024-24995, CVE-2024-24996, CVE-2024-24997, CVE-2024-24998, CVE-2024-24999, CVE-2024-25000, CVE-2024-27975, CVE-2024-27976, CVE-2024-27977, CVE-2024-27978, CVE-2024-27984, CVE-2024-29204
- Avalanche 6.4.3 Security Hardening and CVEs addressed
- Ivanti Security Notifications
- VRM Vulnerability Reports