

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Ivanti Avalanche – version 6.4.0 and prior.

Technical Details

An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in service disruption or arbitrary code execution. This is a similar, but different vulnerability than CVE-2023-32560. Effects Avalanche versions 6.4.0 and older.

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-2023-38036
- [Ivanti Security Advisory - Avalanche CVE-2023-38036](#)

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here:

<https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx>

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca