August 13, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of Ivanti published security advisories to address critical vulnerabilities in the following products:

- Ivanti Virtual Traffic Manager – versions 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1 and 22.7R1
- Ivanti Neurons for ITSM – versions 2023.2, 2023.3 and 2023.4
- Ivanti Avalanche – versions 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.4.0, 6.4.1, 6.4.2 and 6.4.3

Technical Details

Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist 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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-7593 CVE-2024-7569 CVE-2024-7570 CVE-2024-38652 CVE-2024-38653 CVE-2024-36136 CVE-2024-37399 CVE-2024-37373
- Security Advisory: Ivanti Virtual Traffic Manager (vTM) (CVE-2024-7593)
- Security Advisory: Ivanti Neurons for ITSM (CVE-2024-7569, CVE-2024-7570)
- Security Advisory Ivanti Avalanche 6.4.4 (CVE-2024-38652, CVE-2024-38653, CVE-2024-36136, CVE-2024-37399, CVE-2024-37373)
- Ivanti Security Advisories