September 11, 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 Ivanti published security advisories to address critical vulnerabilities in the following products:

- Ivanti IWC – versions 10.18.0.0 and prior
- Ivanti Cloud Services Appliance (CSA) – version CSA 4.6 (versions prior to Patch 519)
- Ivanti Endpoint Manager – version 2024 and versions 2022 SU5 and prior

Technical Details

Ivanti has released an early access version of a new product architecture for Ivanti Workspace Control (IWC) which addresses high and critical vulnerabilities. Successful exploitation could lead to an escalation of privileges and lateral movement. IWC is intended to be a non-internet facing product, and admin privileges are required to exploit these vulnerabilities.

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-2024-37397 CVE-2024-8191 CVE-2024-32840 CVE-2024-32842 CVE-2024-32843 CVE-2024-32845 CVE-2024-32846 CVE-2024-32848 CVE-2024-34779 CVE-2024-34783 CVE-2024-34785 CVE-2024-8320 CVE-2024-8321 CVE-2024-8322 CVE-2024-29847 CVE-2024-8441 CVE-2024-8190
- Security Advisory: Ivanti Workspace Control (IWC)
- Security Advisory: EPM September 2024 for EPM 2024 and EPM 2022
- Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)
- Ivanti Security Advisories