May 22, 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 Ivanti published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Ivanti Connect Secure (ICS) – versions 9.x and 22.x
- Ivanti Endpoint Manager (EPM) – version 2022 SU5 and prior
- Ivanti Neurons for ITSM/ITAM – versions 2023.4, 2023.3, 2023.2 and 2023.1
- Ivanti Policy Secure gateways – versions prior to 22.7R1
- Ivanti Secure Access – versions prior to 22.7R1

Technical Details

An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.

This vulnerability is rated as a **CRITICAL** risk. A software update exists 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.

References

- CVE-2024-29822 CVE-2024-29823 CVE-2024-29824 CVE-2024-29825 CVE-2024-29826 CVE-2024-29827 CVE-2024-29828 CVE-2024-29829 CVE-2024-29830 CVE-2024-29846 CVE-2024-22059 CVE-2024-22060 CVE-2023-38551
- KB Security Advisory Ivanti Secure Access Client May 2024
- KB Security Advisory EPM May 2024
- KB: CVE-2024-22059 and CVE-2024-22060 for Ivanti Neurons for ITSM
- KB Security Advisory Ivanti Connect Secure & Ivanti Policy Secure May 2024
- Ivanti Security Advisories