April 3, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Ivanti published a security advisory to address vulnerabilities in the following products:

- Ivanti Connect Secure (9.x and 22.x) – all versions
- Ivanti Policy Secure Gateway (9.x and 22.x) – all versions

.

Technical Details

A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-21894 CVE-2024-22052 CVE-2024-22053 CVE-2024-22023
- Ivanti Security Advisory
- Ivanti Security Advisories