January 31, 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 (ICS) gateway – versions 9.x and 22.x
- Ivanti Policy Secure (ICS) gateway – versions 9.x and 22.x
- ZTA – version 22.x

Exploitation of these vulnerabilities could allow for privilege escalation and server-side request forgery (SSRF).
Ivanti has indicated that CVE-2024-21893 has been actively exploited.

Technical Details

CVE-2024-21888	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator.	8.8
CVE-2024-21893	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.	8.2

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-2024-21888, CVE-2024-21893
- Ivanti Security Advisory – CVE-2023-21888
- Ivanti Security Advisories