January 10, 2024

**Overall rating: Critical**

**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

Exploitation of these vulnerabilities could allow for authentication bypass and execution of arbitrary commands.
Ivanti has indicated that CVE-2023-46805 and CVE-2024-21887 have been actively exploited.

## Technical Details

A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

These vulnerabilities are rated as an overall **Critical** 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-2023-46805 and CVE-2024-21887
- Ivanti Security Advisory – CVE-2023-46805-CVE-2024-21887
- Ivanti Security Advisories