TIGR Threat Bulletin

SecurityRisk ADVISORS

Ivanti Connect Secure VPN Vulnerability

January 11, 2024

Executive Summary

Security researchers have identified active exploitation of two zero-day vulnerabilities in Ivanti Connect Secure VPN devices, allowing unauthenticated remote code execution. These vulnerabilities, identified as CVE-2023-46805 (authentication-bypass) and CVE-2024-21887 (command-injection), were exploited by attackers for command execution on the VPN appliance. The attackers utilized these vulnerabilities to steal data, modify files, and gain extensive network access. Ivanti has released an official security advisory and mitigation steps, but these do not address past or ongoing compromises. The threat actor, suspected to be a nation-state-level actor, is tracked as UTA0178.

Impact

The exploitation of these vulnerabilities can lead to extensive network breaches, data theft, and unauthorized system access. This poses a significant threat to organizations using Ivanti Connect Secure VPN, especially considering the high CVSS scores of the vulnerabilities (8.2 & 9.1). The attack's sophistication indicates a high level of threat capability, with potential nation-state involvement.

Affected Products

Vulnerabilities have been discovered in Ivanti Connect Secure (ICS), formerly known as Pulse Connect Secure and Ivanti Policy Secure gateways. These vulnerabilities impact all supported versions – Version 9.x and 22.x (refer to Granular Software Release EOL Timelines and Support Matrix for supported versions).

Safeguards/Recommendations

Organizations using Ivanti Connect Secure VPN and Ivanti Policy Secure gateways should immediately apply the mitigation measures provided in Ivanti's KB article as patch development is underway. Patches will be released in a staggered schedule with the first version targeted to be available to customers the week of 22 January and the final version targeted to be available the week of 19 February. Additionally, organizations using these products should review and complete, where possible, the following:

- Continuously monitor Ivanti's advisory article for further updates, as this is an ongoing incident
- Monitor your environment for known indicators of compromise published by Volexity or other sources
- Network traffic analysis originating from your VPN appliances
- ICS VPN device log analysis, such as identifying wiped or disabled logs, and requests for unusual file paths
- Run and review detections from the in-build Integrity Checker Tool released by Ivanti

References

- https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46805
- https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21887
- https://forums.ivanti.com/s/article/KB44755?language=en_US