January 31, 2024

****

Number: AL24-001
Date: January 31, 2024

Title

GPUs from all major suppliers are vulnerable to new pixel-stealing attack.

Audience

Ivanti Connect Secure and Ivanti Policy Secure gateways zero-day vulne Ivanti Connect Secure and Ivanti Policy Secure gateways zero-day vulnerabilities.

Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients. The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

Details

On January 10, 2024, the Cyber Centre was made aware of an authentication bypass vulnerability (CVE-2023-46805) and a command injection vulnerability (CVE-2024-21887) impacting Ivanti Connect Secure (ICS), formerly known as Pulse Connect Secure, and Ivanti Policy Secure (IPS) gateways. Ivanti published a security advisory to highlight these vulnerabilities[Footnote1].
These vulnerabilities impact all supported versions of the software – versions 9.x and 22.x. To highlight the vulnerabilities, the Cyber Centre released an advisory on January 10, 2024[Footnote2].
As of January 10, Ivanti has stated that patches are still under active development and are not ready for distribution. Ivanti has released mitigation steps to address these vulnerabilities. Ivanti also suggests monitoring their Knowledge Base article for patch availability updates related to support versions of Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS), as they become available[Footnote3].
Ivanti has reported that they are aware of exploitation and have observed evidence of threat actors attempting to manipulate Ivanti's internal integrity checker tool (ICT) which is used to ensure filesystem integrity.
Volexity has published a report with an incident summary and indicators of compromise for activity related to these vulnerabilities[Footnote4].

Update 1

On January 15, 2024, Volexity published a report indicating that widespread exploitation has been detected[Footnote5].
The Cyber Centre is aware of proof-of-concept code available in open source.

On January 16, 2024, Ivanti published new guidance related to recovering from exploitation of these vulnerabilities[Footnote6].
Any organizations with continued external facing access to the vulnerable services should assume full device compromise.

Update 2

On January 31, 2024, Ivanti updated their security advisory to indicate the release of patches for the authentication bypass (CVE-2023-46805) and command injection (CVE-2024-21887) vulnerabilities impacting Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) gateways[Footnote1].
Ivanti also disclosed two additional vulnerabilities affecting their Connect Secure, Policy Secure, and Neurons for ZTA products[Footnote8]. A privilege escalation (CVE-2024-21888) allows a server-side request forgery (CVE-2024-21893) in the SAML component and allows a threat actor to access certain restricted resources without authentication. Fixes for these new vulnerabilities are also included in the recently published patches along with new mitigation advice for supported versions where a patch has not been provided[Footnote3] The Cyber Centre has released a security advisory to highlight these additional vulnerabilities[Footnote9].
On January 31, 2024, Mandiant published a blog detailing additional tactics, techniques, and procedures (TTPs) detailing post-exploitation activity and have published indicators of compromise and signatures to aid in the detection of compromise[Footnote10].

References

Footnote 1

CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways

Footnote 2

CCCS AV24-20 – Ivanti security advisory

Footnote 3

KB - CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways

Footnote 4

Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

Footnote 5

Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)

Footnote 6

Recovery Steps Related to CVE-2023-46805 and CVE-2024-21887
Return to footnote6referrer

Footnote 7

Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)

****