
CYBER THREAT INTELLIGENCE ANALYSIS

# THREAT INTELLIGENCE ASSESSMENT

## IVANTI MULTIPLE ZERO-DAY VULNERABILITIES

DOCUMENT PREPARED BY

ELLEN HALLAM
SENIOR THREAT INTELLIGENCE ANALYST

CREATED: 6TH FEBRUARY 2024

# SUMMARY:

A Chinese hacking group, motivated by espionage, exploited vulnerabilities in Ivanti Connect Secure VPN, to gain access to Ivanti VPN appliances. Initial activity was observed from 3rd December 2023.
The vulnerabilities have already been exploited in the wild at the time of publishing, and because an official patch hasn't yet been released these are considered as zero-day vulnerabilities. These vulnerabilities include an authentication bypass vulnerability (CVE-2023-46805) and a command injection vulnerability (CVE-2024-21887) in Connect Secure and Policy Secure gateways, and a critical remote code execution (RCE) vulnerability (CVE-2023-39336) in Endpoint Management software.
If successfully exploited, a cyber threat actor could use these vulnerabilities to take control of an affected system.

# OBSERVATION:

Ivanti have also announced the discovery of two more vulnerabilities:

1. CVE-2024-21893, which is known to be exploited in the wild and which allows an attacker to access certain restricted resources without authentication.
2. CVE-2024-21888, which has not yet been seen to be exploited but allows a user to elevate privileges to that of an administrator.
3. ***Addition**** - Ivanti have also identified a new vulnerability, tracked as CVE-2024-22024, impacting "a limited number of supported versions" of Connect Secure, Policy Secure and Zero Trust Access Gateways. This bug can be used by malicious actors to bypass authentication and "access certain restricted resources." The flaw has a "high" severity rating and is not *yet* believed to have been exploited in the wild.

The vulnerabilities affect Ivanti Connect Secure VPN (formerly Pulse Secure) and Ivanti Policy Secure appliances and impact **all supported versions** – Version 9.x to 22.x.
These vulnerabilities are severe enough that they caused the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to publish an emergency directive, suggesting that the vulnerabilities are being exploited by multiple threat actors. The products are used across the globe, and are vulnerable to successful compromise, with mitigations that are complex to implement.

# ANALYST COMMENT:

Based on the Involvement of the CISA, the vulnerabilities identified are being actively exploited by significant threat actors, suggesting the potential to cause significant damage to Organisations. Although the initial threat actor appears to be an Advanced Persistent Threat which is state-backed, Cybercriminals, who want to conduct more than just cyber espionage are likely to utilise these known vulnerabilities for criminal gain. It is therefore *highly recommended that patches are installed as soon as possible to mitigate risks as soon as they are released.*

# CUSTOMER ACTIONS:

Alongside CISA Supplementary direction, (for CVE-2023-21888 and CVE-2023-21893) Bytes recommend:

1. Disconnect all instances of Ivanti Connect Secure and Ivanti Policy Secure Solutions from Agency networks.
2. Ivanti recommends users performing a factory reset on their appliances, before applying the patch. This precautionary step aims to prevent potential threat actors from gaining upgrade persistence in the environment.
3. Ivanti has released a patch on the 31st January 2024, to cover the initial two vulnerabilities, so this should be applied as soon as possible, to secure systems.

For all discovered issues:

1. Prioritise segmentation of all potentially impacted systems from enterprise resources to reduce the blast radius.
2. Continuous Threat-hunting activity for all devices connected to and from the impacted Ivanti products.
3. Monitoring of Identity management services and authentication anomalies.
4. Active audit of privileged accounts that were recently created or updated.
5. Rotate certificates, keys, and passwords for all connected or exposed systems and applications.

*Caveat:* This is based on current, limited, knowledge, which should be further investigated and checked, before being applied to your systems.

## SOURCES:


1. Ivanti VPN vulnerability: How to defend against CVE-2023-46805, CVE-2024-21887 (skyboxsecurity.com)
2. Supplemental Direction V1: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities | CISA
3. Replace Ivanti VPN with Netskope ZTNA Next - Netskope
4. Get help for the Ivanti VPN exploit (paloaltonetworks.com)
5. CVE-2024-22024 (XXE) for Ivanti Connect Secure and Ivanti Policy Secure