

Addendum to Feb 2024 advisory on “Adversaries exploit Ivanti’s zero-day vulnerabilities”

Original report published on: 29 Feb, 2024

Updated on: 03 Apr, 2024^[1]

Executive Summary

On 2 April 2024, Ivanti identified four additional vulnerabilities (CVE-2024-21894, CVE-2024-22052, CVE-2024-22053 and CVE-2024-22023) in Ivanti Connect Secure and Ivanti Policy Secure gateways.

For organisations that rely on Ivanti for secure remote access, these vulnerabilities could disrupt services and compromise sensitive data if exploited. Ivanti has released a patch on 3 April 2024 to address these vulnerabilities.

Ivanti indicated that there is no evidence of these vulnerabilities being exploited in the wild and that there is no impact to any other Ivanti products or solutions.

Background

Adversaries can exploit vulnerabilities such as heap overflow, null pointer dereference, improper check for unusual exceptional conditions and XML External Entity Expansion (XEE) to achieve remote code execution (RCE) and conduct a denial-of-service (DoS). In certain conditions, it may also lead to execution of arbitrary code.

Details of the vulnerabilities^[2]

- a. CVE-2024-21894 – Heap Overflow Vulnerability
 - i. Successful exploitation allows an unauthenticated attacker to send specially crafted requests in-order-to crash the service thereby causing a denial of service (DoS) attack, or in certain conditions lead to execution of arbitrary code, due to a heap overflow vulnerability in the IPsec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure.
 - ii. The CVSS is rated high and scored at 8.2.
- b. CVE-2024-22052 – Null Pointer Dereference Vulnerability
 - i. Successful exploitation allows an unauthenticated attacker to send specially crafted requests in-order-to crash the service thereby causing a DoS due to a null pointer dereference vulnerability in the IPsec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure.
 - ii. The CVSS is rated high and scored at 7.5.
- c. CVE-2024-22053 – Heap Overflow Vulnerability

- i. Successful exploitation allows an unauthenticated attacker to send specially crafted requests in-order-to crash the service thereby causing a DoS, or in certain conditions read contents from memory, due to a heap overflow vulnerability in the IPsec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure.
 - ii. The CVSS is rated high and scored at 8.2.
- d. CVE-2024-22023 – XML Entity Expansion Vulnerability
- i. Successful exploitation allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS due to an XML entity expansion (XEE) vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure.
 - ii. The CVSS is rated medium and scored at 5.3.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Organisations using Ivanti Connect Secure and Policy Secure gateways are strongly advised to apply the patch released on 3rd April immediately to fix these vulnerabilities and prevent potential attacks by malicious actors.
- Refer to the MITRE ATT&CK techniques and validate security controls to create detection rules and deny processes related to these techniques if there is no business need.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

MITRE ATT&CK Tactics and Techniques

Initial Access		
Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Adversaries send specially crafted requests to the vulnerable Ivanti Connect Secure and Policy Secure gateways to achieve RCE and conduct a denial-of-service DoS attack.
Lateral Movement		
Remote Services	T1021	Adversaries exploit the vulnerabilities to conduct RCE.
Execution		
Technique Title	ID	Use

Exploitation for Client Execution	T1203	Adversaries can take advantage of CVE-2024-21894 vulnerabilities through targeted exploitation for the purpose of arbitrary code execution.
Impact		
Network Denial of Service	T1498	Adversaries exploit the vulnerabilities to conduct DoS attack.

References

1. [^ "Security Update for Ivanti Connect Secure and Policy Secure"](#).
2. [^ "New CVE-2024-21894 \(Heap Overflow\), CVE-2024-22052 \(Null Pointer Dereference\), CVE-2024-22053 \(Heap Overflow\), CVE-2024-22023 \(XML entity expansion or XXE\) and CVE-2024-29205 for Ivanti Connect Secure and Ivanti Policy Secure Gateways"](#).