

HiveForce Labs

# THREAT ADVISORY

 VULNERABILITY REPORT

## Ivanti Addresses Yet Another VPN Flaw Within a Month

Date of Publication

February 9, 2024

Admiralty Code

A1

TA Number

TA2024051




# Summary

**First Seen:** February 8, 2024

**Affected Products:** Ivanti Connect Secure, Policy Secure, and ZTA gateway

**Impact:** Ivanti has addressed a newly discovered vulnerability impacting ZTA, Policy, and Connect Secure gateways. Tracked as CVE-2024-22024, this vulnerability stems from a weakness in the SAML component of the gateways related to XXE (XML eXternal Entities), enabling remote attackers to access restricted resources.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-22024	Ivanti Connect Secure, Policy Secure, and ZTA XML external entity or XXE Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways			

# Vulnerability Details

## #1

Ivanti has flagged a new high-severity vulnerability, designated CVE-2024-22024, impacting the Connect Secure, Policy Secure, and ZTA gateways. This vulnerability originates from a weakness related to XXE (XML external Entities) in the SAML component of the gateways. It permits remote attackers to access restricted resources on vulnerable appliances without user interaction or authentication.

## #2

The vulnerability CVE-2024-22024 enables remote attackers to access and manipulate data on the affected system. This vulnerability arises from insufficient validation of XML input provided by users. By crafting customized XML code, a remote attacker can retrieve the contents of any file on the system and modify stored data as desired.

## #3

A select range of supported versions, including ZTA, Ivanti Policy Secure, and Ivanti Connect Secure, are impacted by the CVE-2024-22024 vulnerability. Ivanti has clarified that there is currently no indication of any customers falling victim to exploitation by this vulnerability. Ivanti has released patches and has also provided mitigations, however applying mitigations may degrade certain features.

## #4

Since December 2023, there have been attacks targeting Ivanti VPN appliances utilizing zero-day vulnerabilities, namely [CVE-2023-46805](#) for authentication bypass and [CVE-2024-21887](#) for command injection. Additionally, a third zero-day vulnerability, [CVE-2024-21893](#), involving server-side request forgery, has been actively exploited.

## #5

In light of pervasive targeting by various threat actors, CISA issued a directive on February 1, instructing U.S. federal agencies to disconnect all susceptible Ivanti VPN appliances from their networks within 48 hours. Ivanti promptly responded by releasing security patches for the three vulnerabilities on January 31. Customers who applied the patch released on January 31 or February 1, along with completing a factory reset of their appliance, are exempt from further reset requirements.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-22024	Ivanti Connect Secure (version 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 and 22.5R1.1), Ivanti Policy Secure version 22.5R1.1 and ZTA version 22.6R1.3	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*	CWE-611

## Recommendations



**Apply Patch:** Install the security patch provided by Ivanti to address the CVE-2024-22024 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.



**Least Privilege:** Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.



**Deploy Anomaly Detection and Monitoring:** Implement network monitoring tools with anomaly detection capabilities to identify unusual or suspicious patterns of network activity. This can include unexpected increases in data traffic, unusual access patterns, or deviations from normal behavior.

# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1190</u></b> Exploit Public-Facing Application		

## Patch Details

Ivanti has released patches to address the vulnerability in the following product versions:

Ivanti Connect Secure versions 9.1R14.5, 9.1R17.3, 9.1R18.4, 22.4R2.3, 22.5R1.2, 22.5R2.3 and 22.6R2.2

Ivanti Policy Secure versions 9.1R17.3, 9.1R18.4 and 22.5R1.2

ZTA gateways versions 22.5R1.6, 22.6R1.5 and 22.6R1.7

Link:

<https://forums.ivanti.com/s/product-downloads/>

To mitigate CVE-2024-22024, you can import the mitigation.release.20240126.5.xml file through the download portal.

## References

[https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en\\_US](https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US)

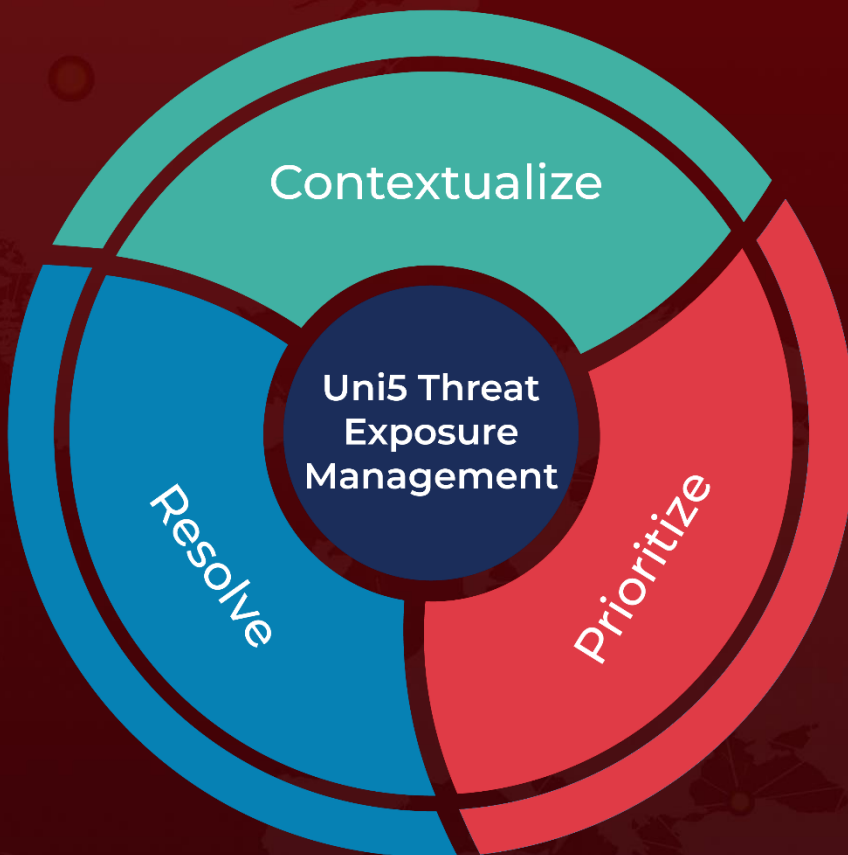
<https://www.hivepro.com/threat-advisory/two-zero-day-flaws-found-in-ivanti-connect-secure-and-policy-secure/>

<https://www.hivepro.com/threat-advisory/ivanti-addresses-zero-day-vulnerability-exploited-in-attacks/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**February 9, 2024 • 4:25 AM**

© 2024 All Rights are Reserved by Hive Pro®



More at [www.hivepro.com](http://www.hivepro.com)