

Hiveforce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Ivanti Addresses Flaws Leading to DoS Attacks and Code Execution

Date of Publication

April 5, 2024

Admiralty Code

A1

TA Number

TA2024132













Summary

First Discovered: April 2024

Affected Product: Ivanti Connect Secure (ICS) and Ivanti Policy Secure gateways

Impact: Ivanti has discovered four security vulnerabilities in Connect Secure and Policy Secure Gateways, designated as CVE-2024-21894, CVE-2024-22052, CVE-2024-22053, and CVE-2024-22023. These vulnerabilities pose significant risks as they could potentially enable threat actors to conduct denial-of-service (DoS) attacks or execute arbitrary code.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-21894	Ivanti Heap Overflow Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure			
CVE-2024-22052	Ivanti Null Pointer Dereference vulnerability	Ivanti Connect Secure and Ivanti Policy Secure			
CVE-2024-22053	Ivanti Heap Overflow Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure			
CVE-2024-22023	Ivanti XML Entity Expansion or XEE Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure			

Vulnerability Details

#1

Ivanti has released patches to mitigate several security vulnerabilities, including CVE-2024-21894, CVE-2024-22052, CVE-2024-22053, and CVE-2024-22023, affecting its Connect Secure and Policy Secure gateways. These vulnerabilities could enable threat actors to execute arbitrary code and carry out denial-of-service (DoS) attacks.

#2

CVE-2024-21894 is a vulnerability identified in the IPSec component, characterized by a boundary error. This flaw can be exploited by an attacker sending specifically crafted packets to the targeted device. Upon successful exploitation, a heap-based buffer overflow occurs, allowing the attacker to execute arbitrary code on the vulnerable system.

#3

CVE-2024-22052 pertains to an issue where a malicious user can send specifically crafted queries to the IPSec component. This vulnerability has the potential to result in a null pointer dereference vulnerability, which could lead to a DoS attack. On the other hand, CVE-2024-22053 is a heap overflow vulnerability discovered in the IPSec component. In this scenario, an unauthenticated user could exploit the vulnerability, potentially causing service crashes. Additionally, under certain conditions, this flaw might allow the attacker to read memory contents.

#4

CVE-2024-22023 relates to a vulnerability in the SAML component where user-supplied XML input is not adequately validated. This oversight allows a remote attacker to exploit the system by sending specifically crafted XML data, leading to resource depletion and causing a temporary DoS condition.

#5

Although there have been no reported exploits of these vulnerabilities at present, it's important to highlight that Nation-state actors have targeted Ivanti software with multiple vulnerabilities throughout the year. Therefore, administrators are strongly advised to apply the available patches promptly to address these vulnerabilities and enhance the security of their systems against potential exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21894	Ivanti Connect Secure and Ivanti Policy Secure All Version of 9.x and 22.x	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*	CWE-122
CVE-2024-22052			CWE-476
CVE-2024-22053			CWE-122
CVE-2024-22023			CWE-611

Recommendations



Apply Patch: Install the security patch provided by Ivanti to address the CVE-2024-21894, CVE-2024-22052, CVE-2024-22053, and CVE-2024-22023 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.



Monitor Traffic Patterns: Monitor network traffic patterns regularly to detect any abnormal behavior that may indicate a potential DoS attack. Use monitoring tools and set up alerts to notify you of suspicious activity.



Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0040</u> Impact	<u>T1588</u> Obtain Capabilities
<u>T1588.006</u> Vulnerabilities	<u>T1498</u> Network Denial of Service	<u>T1059</u> Command and Scripting Interpreter	<u>T1499</u> Endpoint Denial of Service

Patch Details

Patch is now available for all supported versions of the product through the Ivanti download portal. Upgrade to the below patched version.

Ivanti Connect Secure: 22.1R6.2, 22.2R4.2, 22.3R1.2, 22.4R1.2, 22.4R2.4, 22.5R1.3, 22.5R2.4, 22.6R2.3, 9.1R14.6, 9.1R15.4, 9.1R16.4, 9.1R17.4 and 9.1R18.5

Ivanti Policy Secure: 22.4R1.2, 22.5R1.3, 22.6R1.2, 9.1R16.4, 9.1R17.4 and 9.1R18.5

Link: <https://forums.ivanti.com/s/article/New-CVE-2024-21894-Heap-Overflow-CVE-2024-22052-Null-Pointer-Dereference-CVE-2024-22053-Heap-Overflow-and-CVE-2024-22023-XML-entity-expansion-or-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways>

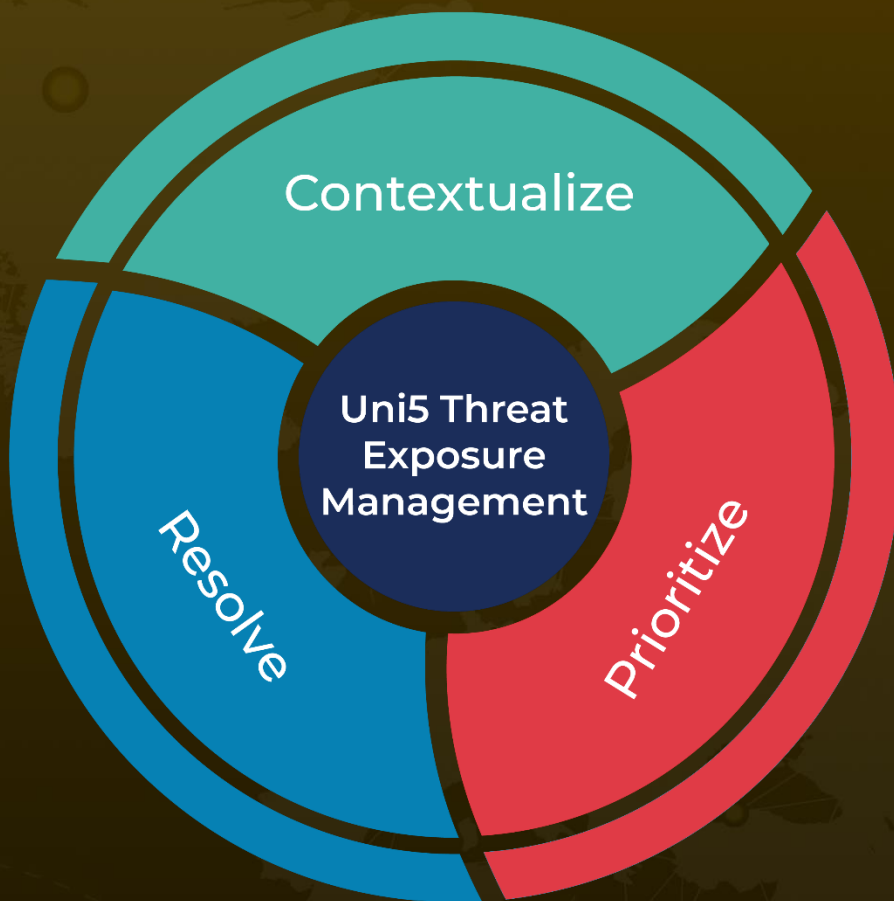
References

https://forums.ivanti.com/s/article/SA-CVE-2024-21894-Heap-Overflow-CVE-2024-22052-Null-Pointer-Dereference-CVE-2024-22053-Heap-Overflow-and-CVE-2024-22023-XML-entity-expansion-or-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

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

April 5, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com