Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ivanti Addresses Zero-Day Vulnerability Exploited in Attacks

Date of Publication	Last Update Date	Admiralty Code	TA Number
February 2, 2024	February 14, 2024	A1	TA2024042

Summary

First Seen: February 2024
Affected Products: Connect Secure, Policy Secure, and Ivanti Neurons for ZTA
Malware: DSLog backdoor
Impact: Ivanti has addressed two new high-severity vulnerabilities, CVE-2024-21893 and CVE-2024-21888, affecting its Connect Secure and Policy Secure products. CVE-2024-21893, in particular, has been actively exploited in the wild, posing a significant risk to affected systems.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA	✓	✓	✓
CVE-2024-21888	Ivanti Privilege Escalation Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure	✗	✗	✓

Vulnerability Details

#1 Ivanti has released fixes for high-severity vulnerabilities impacting its Connect Secure and Policy Secure products. Among the identified vulnerabilities is a zero-day flaw, CVE-2024-21893, which enables attackers to access restricted resources without authentication. CVE-2024-21888 permits users to elevate their privileges to administrator level.

#2 CVE-2024-21888 stems from inadequately enforced security restrictions within the web interface. This flaw enables a remote user to circumvent these restrictions and attain administrative privileges.

#3 CVE-2024-21893 enables remote attackers to conduct SSRF attacks by exploiting insufficient validation of user-provided information in the SAML component. By crafting a specially designed request, attackers can deceive the application into sending requests to any system and access sensitive data within the local network. It's crucial to note that this vulnerability is actively being exploited in the wild.

#4 Threat actors are installing a backdoor called DSLog on susceptible devices by taking advantage of this vulnerability. Through encoded commands included in SAML authentication requests, this backdoor was added to the appliance's code base. The purpose of the SAML requests was to detect any changes made to a legal logging script (DSLog.pm), detect read/write filesystem permissions on the infected device, and inject the backdoor if the modification indicator was missing.

#5 The backdoor is introduced in the DSLog file, which records system logs and authenticated web requests. Embedding backdoor in DSLog file enables attacker to execute any commands with root privileges through simple HTTP requests. About 700 Ivanti servers were hacked. Of these endpoints, 20% had previously been impacted by prior campaigns, while the remaining endpoints became exposed because there were no patches or mitigations in place.

#6 Ivanti has also released patches for two other zero-day vulnerabilities disclosed in early January: **CVE-2023-46805 and CVE-2024-21887**. These vulnerabilities have been chained together in widespread attacks aimed at deploying malware on vulnerable ICS, IPS, and ZTA gateways, and it is crucial for users and organizations to apply them promptly to mitigate the risk of exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21893	Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x, ZTA gateways: Version 9.x and 22.x	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	CWE-918
CVE-2024-21888	Pulse Connect Secure: Version 9.x and 22.x, Pulse Policy Secure: Version 9.x and 22.x	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	CWE-264

Recommendations

Apply Patch: Install the security patch provided by Ivanti to address the CVE-2024-21893 and CVE-2024-21888 vulnerabilities. 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.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
Filename	/root/home/webserver/htdocs/dana-na/imgs/index[.]txt, /root/home/webserver/htdocs/dana-na/imgs/index1[.]txt, /root/home/webserver/htdocs/dana-na/imgs/index2[.]txt, /root/home/webserver/htdocs/dana-na/imgs/index2[.]txt
IP	159.65.123[.]122

Patch Details

Ivanti has released patches to address all identified vulnerabilities in the following product versions:
Ivanti Connect Secure: Versions 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2, 22.5R1.1, and 22.5R2.2
Ivanti Policy Secure: Version 22.5R1.1
ZTA: Version 22.6R1.3

Link:
https://forums.ivanti.com/s/product-downloads/

References

https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

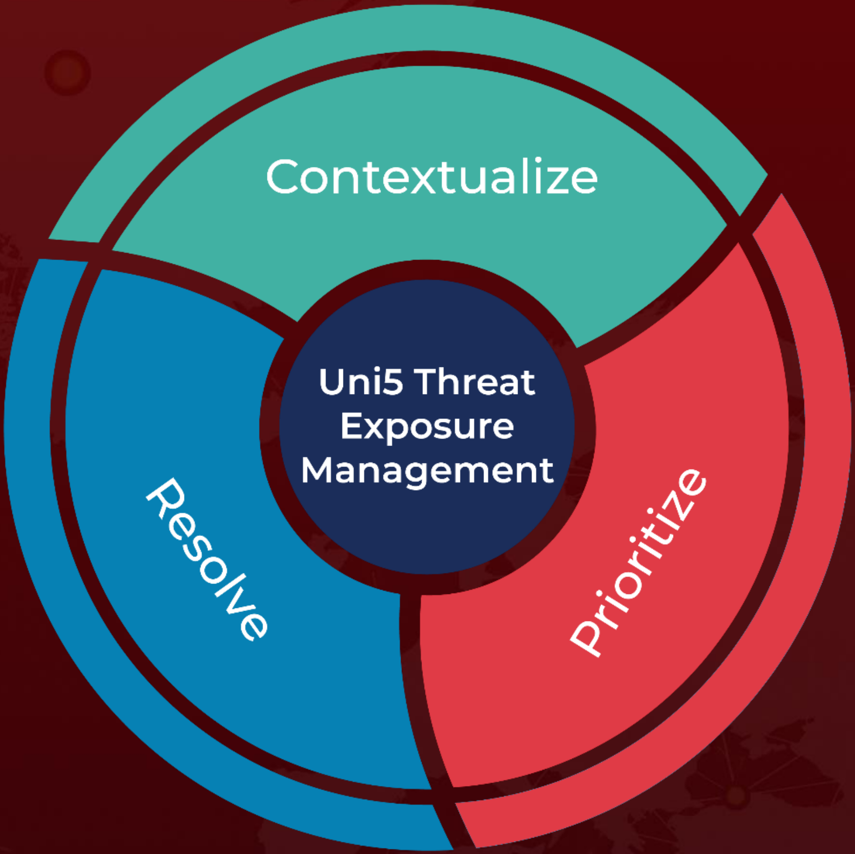
https://www.hivepro.com/threat-advisory/two-zero-day-flaws-found-in-ivanti-connect-secure-and-policy-secure/

https://www.orangecyberdefense.com/global/blog/research/ivanti-connect-secure-journey-to-the-core-of-the-dslog-backdoor

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 2, 2024 • 5:20 AM

More at www.hivepro.com