Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Two Zero-Day Flaws Found in Ivanti Connect Secure and Policy Secure

Date of Publication	Last updated date	Admiralty Code	TA Number
January 11, 2024	April 24, 2024	A1	TA2024011

Summary

First Seen: December 2023
Affected Platform: Ivanti Connect Secure and Ivanti Policy Secure
Targeted Industries: Government, Military, Telecommunications, Defense, Technology, Banking, Finance, Accounting, Aerospace, Aviation, Engineering
Malware: Giftedvisitor, Zipline Passive Backdoor, Thinspool Dropper, Wirefire web shell, Lightwire web shell, Warpwire harvester, PySoxy tunneler, and Thinspool
Impact: The active exploitation of zero-day vulnerabilities (CVE-2023-46805 and CVE-2024-21887) in Ivanti Connect Secure and Ivanti Policy Secure gateways presents a serious threat, allowing unauthorized remote code execution. The actor, recognized as the Chinese nation-state-level entity UTA0178 or UNC5221, employed these exploits for system compromise, underscoring the urgency for affected organizations to promptly apply mitigations, conduct comprehensive post-compromise analyses, and implement forthcoming patches.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure	✓	✓	✓

Vulnerability Details

#1

Two critical zero-day vulnerabilities (CVE-2023-46805 and CVE-2024-21887) in Ivanti Connect Secure (ICS) and Ivanti Policy Secure gateways, affecting all supported versions, have been identified. When exploited together, these vulnerabilities could lead to unauthenticated remote code execution. Ivanti Neurons for ZTA gateways are vulnerable if generated but not connected to a ZTA controller.

#2

The threat actor, identified as UTA0178 or UNC5221, a suspected Chinese nation-state-level actor, executed various activities, including stealing configuration data and establishing reverse tunnels, leveraging the compromised VPN appliances. The attacker used the webshell named GLASSTOKEN for persistence and command execution, modifying legitimate components for evasion and credential exfiltration.

#3

As of January 14, over 1,700 ICS VPN appliances have been compromised globally, impacting multiple sectors. The tools used in the attacks include Zipline Passive Backdoor, Thinspool Dropper, Wirefire web shell, Lightwire web shell, Warpwire harvester, PySoxy tunneler, and Thinspool utility.

#4

In January 2024, MITRE Corporation fell victim to a nation-state actor exploiting these Ivanti software flaws to breach their unclassified research network NERVE. Although the attackers accessed the network and deployed data extraction tools, there's no evidence to suggest MITRE's main network or partners were affected.

#5

Ivanti's internal integrity checker has been targeted, prompting the recommendation for customers to run the external integrity checker. The impact includes the degradation of various features like Admin REST APIs, automation, End User Portal functionality, and Citrix StoreFront with HTML5.

#6

A workaround involves importing the mitigation.release.20240107.1.xml file. Patches for supported versions were made available in the first week of February. While Ivanti advises applying the provided mitigation immediately, it emphasizes that mitigation does not address past compromises. Previous zero-day vulnerabilities exploited by state-affiliated hackers in Ivanti's products for cyberattacks, including in Ivanti Endpoint Manager Mobile (EPMM) and Ivanti Sentry.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-46805	Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	CWE-287
CVE-2024-21887	Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply Mitigation: Import the mitigation.release.20240107.1.xml file via the download portal to address the vulnerabilities temporarily. Organizations are strongly advised to apply this mitigation immediately to reduce the risk of exploitation. Once patches for the identified vulnerabilities are released, promptly update and patch the affected Ivanti gateways.

Run External Integrity Checker: Due to threat actors targeting Ivanti's internal integrity checker, all customers are recommended to run the external integrity checker. The external integrity checker can provide an additional layer of security and help identify potential compromises.

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.

Network Segmentation: Employ network segmentation to isolate email security appliances from critical internal networks. This can help contain the impact of a potential breach and prevent lateral movement within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration	TA0008 Lateral Movement
TA0042 Resource Development	TA0043 Reconnaissance	TA0011 Command and Control	TA0003 Persistence
T1056 Input Capture	T1056.001 Keylogging	T1059.007 JavaScript	T1059 Command and Scripting Interpreter
T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1588.006 Vulnerabilities	T1659 Content Injection
T1059.001 PowerShell	T1589.001 Credentials	T1589 Gather Victim Identity Information	T1588.005 Exploits

T1572 Protocol Tunneling	**T1059.006** Python	**T1090** Proxy	**T1505.003** Web Shell
T1505 Server Software Component	**T1588** Obtain Capabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	206[.]189[.]208[.]156, 75[.]145[.]243[.]85, 47[.]207[.]9[.]89, 98[.]160[.]48[.]170, 173[.]220[.]106[.]166, 73[.]128[.]178[.]221, 50[.]243[.]177[.]161, 50[.]213[.]208[.]89, 64[.]24[.]179[.]210, 75[.]145[.]224[.]109, 50[.]215[.]39[.]49, 71[.]127[.]149[.]194, 173[.]53[.]43[.]7
Hostnames	gpoaccess[.]com, webb-institute[.]com, symantke[.]com
FileNames	compcheckresult[.]cgi, sessionserver[.]sh, lastauthserverused[.]js, visits[.]py, sessionserver[.]pl, libsecure[.]so[.]1
MD5	3d97f55a03ceb4f71671aa2ecf5b24e9, 677c1aa6e2503b56fe13e1568a814754, 6de651357a15efd01db4e658249d4981, d0c7a334a4d9dcd3c6335ae13bee59ea
SHA256	8bc8f4da98ee05c9d403d2cb76097818de0b524d90bea8ed846615e42cb031d2, 26cbb54b1feb75fe008e36285334d747428f80aacdb57badf294e597f3e9430d, 9d901f1a494ffa98d967ee6ee30a46402c12a807ce425d5f51252eb69941d988, E192932d834292478c9b1032543c53edfc2b252fdf7e27e4c438f4b249544eeb

Patch Link

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

References

https://www.cisa.gov/news-events/alerts/2024/01/10/ivanti-releases-security-update-connect-secure-and-policy-secure-gateways

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

https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

https://www.hivepro.com/threat-advisory/ivanti-addressed-second-zero-day-flaw-exploited-by-attackers/

https://www.hivepro.com/threat-advisory/ivanti-addressed-a-new-zero-day-flaw-in-ivanti-sentry/

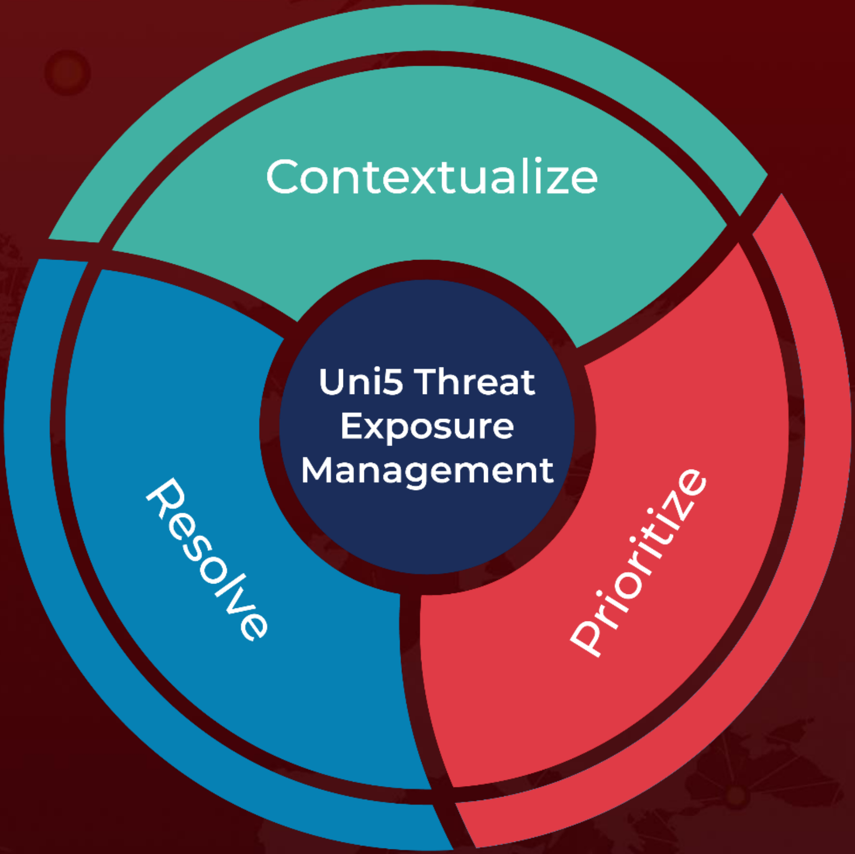
https://www.mitre.org/news-insights/news-release/mitre-response-cyber-attack-one-its-rd-networks

https://medium.com/mitre-engenuity/advanced-cyber-threats-impact-even-the-most-prepared-56444e980dc8

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

January 11, 2024 • 6:30 AM

More at www.hivepro.com