Hive Pro®

Threat Level

Red

CISA: AA24-060B

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

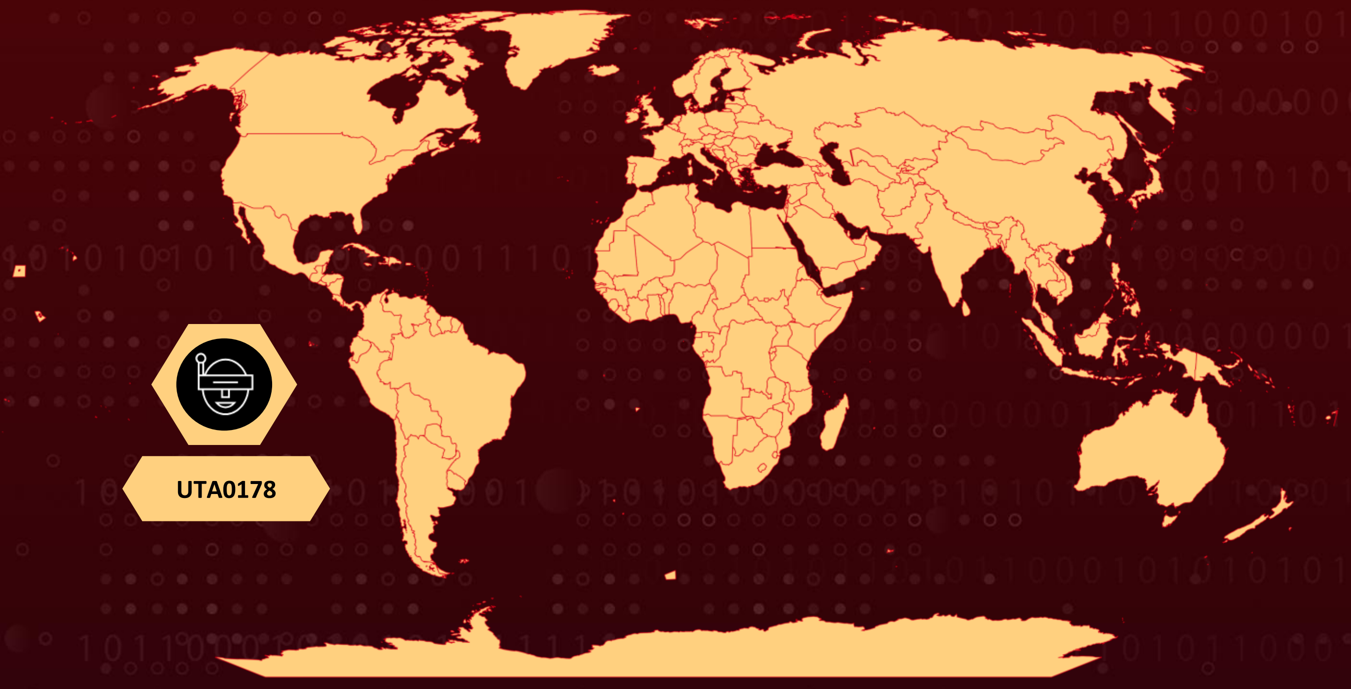
Ivanti Gateways Under Attack by Cybercriminals Patch Now

Date of Publication	Admiralty Code	TA Number
March 1, 2024	A1	TA2024082

Summary

Attack Observed: February 29, 2024
Targeted countries: Worldwide
Threat Actor: UTA0178
Targeted Industries: Government, Military, Telecommunications, Defense, Technology, Banking, Finance, Accounting, Aerospace, Aviation, Engineering
Affected Platforms: Ivanti Connect Secure and Ivanti Policy Secure
Attack: Cyber threat actors have been exploiting vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways, including CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893, which allow them to bypass authentication and execute arbitrary commands with elevated privileges. Despite Ivanti's mitigation efforts, threat actors persist, emphasizing the need for immediate patching to protect against these potential exploitation risks.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

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 Policy Secure	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
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-2024-22024	Ivanti Connect Secure, Policy Secure, and ZTA XML external entity or XXE Vulnerability	Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways	☒	☒	✓
CVE-2024-21888	Ivanti Connect Secure and Policy Secure Privilege Escalation Vulnerability	Ivanti Connect Secure and Ivanti Policy Secure	☒	☒	✓

Attack Details

#1 Cyber threat actors have been exploiting vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways, including CVE-2023-46805, CVE-2024-21887, and CVE-2024-21893, which allow them to bypass authentication and execute arbitrary commands with elevated privileges. Despite efforts by Ivanti to mitigate these vulnerabilities, threat actors have developed methods to bypass these mitigations, leading to further exploitation.

#2 On January 10, 2024, two vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways, CVE 2023-46805 and CVE-2024-21887, being chained to achieve unauthenticated remote code execution (RCE). Active exploitation was first observed in early December 2023, leading to the implantation of web shells like GLASSTOKEN and GIFTEDVISITOR on both internal and external-facing servers. These web shells allowed threat actors to execute commands on compromised devices.

#3 Despite initial mitigation guidance from Ivanti, threat actors developed methods to bypass these mitigations, deploying additional web shell variants such as BUSHWALK, LIGHTWIRE, and CHAINLINE. Subsequently, Ivanti disclosed three more vulnerabilities: CVE-2024-21893, CVE-2024-22024, and CVE-2024-21888, which further exposed the gateways to exploitation, including server-side request forgery, XML vulnerabilities, and privilege escalation.

#4 CISA’s incident response engagements have revealed that Ivanti's Integrity Checker Tool (ICT), both internal and external versions, have failed to detect compromises. Even after performing factory resets, cyber threat actors have been able to maintain root-level persistence on compromised devices, rendering the ICT ineffective in identifying compromise. Additionally, forensic analysis has shown that threat actors can manipulate files and system settings to evade detection by ICT scans, creating a false sense of security.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Patch Management: Maintain a rigorous patch management process to ensure that all software, including operating systems, web browsers, and security applications, is up-to-date with the latest security patches. Promptly apply patches released by software vendors to mitigate known vulnerabilities.

Limit Outbound Internet Connections: Restrict outbound internet connections from SSL VPN appliances to only necessary services. This limits the ability of threat actors to download tools or establish connections to command and control servers.

Enforce Strict Access Controls: Configure SSL VPN appliances with Active Directory or LDAP authentication to use low privilege accounts for authentication. Limit SSL VPN connections to unprivileged accounts to minimize exposure of privileged credentials.

Potential MITRE ATT&CK TTPs

TA0008 Lateral Movement	TA0003 Persistence	TA0006 Credential Access	TA0002 Execution
TA0001 Initial Access	TA0042 Resource Development	TA0004 Privilege Escalation	T1505 Server Software Component
T1059 Command and Scripting Interpreter	T1203 Exploitation for Client Execution	T1068 Exploitation for Privilege Escalation	T1059.001 PowerShell
T1588 Obtain Capabilities	T1588.005 Exploits	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application
T1078 Valid Accounts	T1505.003 Web Shell		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ed4b855941d6d7e07aacf016a2402c4c870876a050a4a547af194f5a9b47945f
MD5	3045f5b3d355a9ab26ab6f44cc831a83, 3d97f55a03ceb4f71671aa2ecf5b24e9, 2ec505088b942c234f39a37188e80d7a, 8eb042da6ba683ef1bae460af103cc44, a739bd4c2b9f3679f435797114487 86f, a81813f70151a022ea1065b7f4d6b5ab, d0c7a334a4d9dcd3c6335ae13bee59ea, e8489983d73ed30a4240a14b1f161254
Domain	symantke[.]com, miltonhouse[.]nl, entraide-internationale[.]fr, api.d-n-s[.]name, cpanel.netbar[.]org, clickcom[.]click, clicko[.]click, duorhytm[.]fun,

TYPE	VALUE
Domains	line-api[.]com, areekaweb[.]com, ehangmun[.]com, secure-cama[.]com, gpoaccess[.]com, webb-institute[.]com, symantke[.]com
IPv4	88.119.169[.]227, 103.13.28[.]40, 46.8.68[.]100, 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, 146.0.228[.]66, 159.65.130[.]146, 8.137.112[.]245, 91.92.254[.]14, 186.179.39[.]235 , 50.215.39[.]49, 45.61.136[.]14, 173.220.106[.]166,
File names	Cav-0.1-py3.6.egg, Health.py, compcheckresult.cgi, lastauthserverused.js, logo.gif, login.gif, [a-fA-f0-9]{10\.css, visits.py

TYPE	VALUE
File paths	/home/perl/DSLogConfig.pm, /usr/bin/a.sh, /bin/netmon, /home/venv3/lib/python3.6/site-packages/*.egg, /home/etc/sql/dsserver/sessionserver.pl, /home/etc/sql/dsserver/sessionserver.sh, /home/webserver/htdocs/dana-na/auth/compcheckresult.cgi, /home/webserver/htdocs/dana-na/auth/lastauthserverused.js

Patch Links

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

https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

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

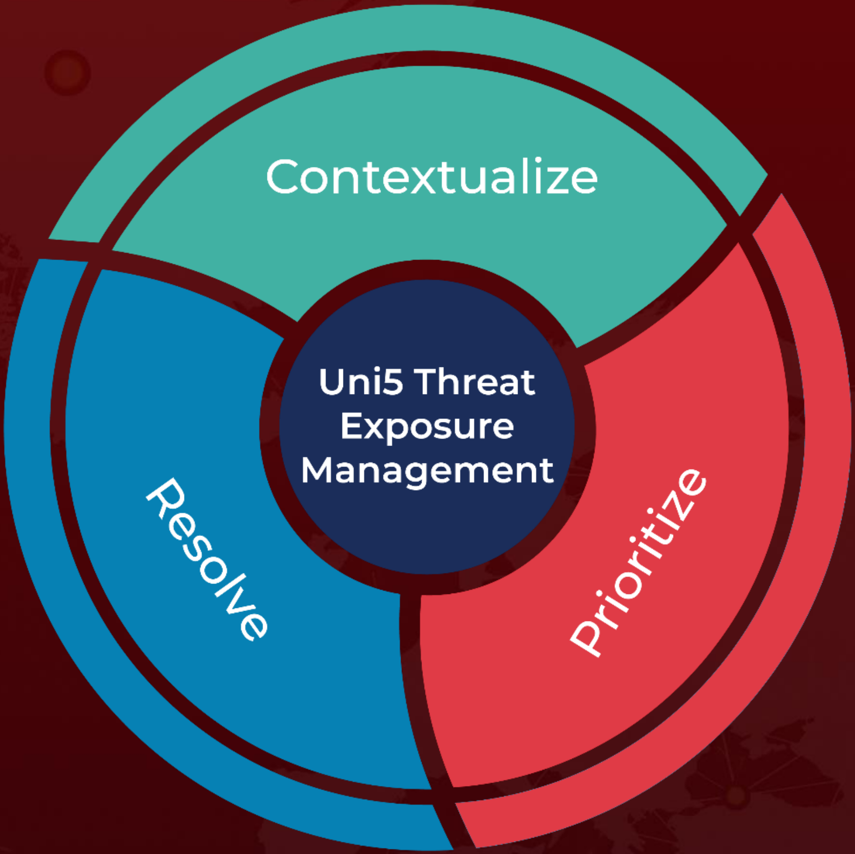
https://www.hivepro.com/threat-advisory/ivanti-addresses-zero-day-vulnerability-exploited-in-attacks/

https://www.hivepro.com/threat-advisory/ivanti-addresses-yet-another-vpn-flaw-within-a-month/

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

March 1, 2024 • 4:30 AM

More at www.hivepro.com