United States Coast Guard (USCG) Cyber Command Maritime Cyber Alert 01-24

March 7, 2024

Information Sharing Protocol: TLP: CLEAR (https://www.us-cert.gov/tlp)

Exploitation of Ivanti Connect Secure and Policy Secure Gateways

Summary:

Marine Transportation System (MTS) entities that use Ivanti Connect Secure and Ivanti Policy Secure solutions are vulnerable to known Common Vulnerability and Exposures (CVEs): CVE-2023-46805, CVE-2024-21887, CVE-2024-21893, CVE-2024-22024, and CVE-2024-21888 impacting all supported versions (9.x and 22.x). These CVEs allow an attacker to bypass control checks and authenticate as an administrator over the internet to move laterally, perform data exfiltration, establish persistent system access, and remotely gain control of the affected system.

Background:

Ivanti Connect Secure is a virtual private network (VPN) security solution that allows web-enabled devices to access corporate resources. Ivanti Policy Secure is a network access control solution that provides network access to authorized and secured users and devices. Vulnerabilities with Ivanti Connect Secure and Ivanti Policy Secure were first observed in early December 2023 and reported in January 2024. Following the identification of these vulnerabilities, Ivanti provided initial mitigation guidance. However, threat actors quickly developed methods to bypass the mitigation measures and began exploiting additional vulnerabilities in the Ivanti products.

The impact of these vulnerabilities is substantial. Ivanti Connect Secure is the most widely used Secure Socket Layer (SSL) VPN across every major industry, for organizations of every size.[1] Additionally, Ivanti serves more than 40,000 customers, including 96 of the Fortune 100

[1]"Ivanti Connect Secure [Datasheet]." *www.ivanti.com*, www.ivanti.com/resources/v/doc/ivi/2516/9c01b1c709cb.

companies.[2] In CISA's most recent cybersecurity advisory published on February 29th, 2024, organizations are strongly urged to:

"Consider the significant risk of adversary access to, and persistence on, Ivanti Connect Secure and Ivanti Policy Secure gateways when determining whether to continue operating these devices in an enterprise environment."[3]

Targeted Applications & Systems:

Cyber threat actors have been actively exploiting multiple vulnerabilities—CVE-2023-46805, CVE-2024-21887, CVE-2024-21893, CVE-2024-22024, and CVE-2024-21888—affecting Ivanti Connect Secure and Ivanti Policy Secure gateways. The vulnerabilities impact all supported versions (9.x and 22.x) and can be used in a chain of exploits to enable malicious actors to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges.

The Ivanti Connect Secure and Ivanti Policy Secure vulnerabilities affect the following versions of the Ivanti gateway software:

- Ivanti Connect Secure 9.x
- Ivanti Connect Secure 22.x
- Ivanti Policy Secure 9.x
- Ivanti Policy Secure 22.x

Threat Actor Tactics:

Below are the tactics referenced by MITRE ATT&CK®[1] techniques, which are linked to these attacks (https://attack.mitre.org/techniques/enterprise):

- **T1190: Exploit Public-Facing Application**
  - An authentication bypass vulnerability in the web component of Ivanti Connect Secure 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.
- **T1078: Valid Accounts**
  - Once access has been gained, attackers are able to move laterally within internal systems through Remote Desktop Protocol (RDP) and Secure Shell (SSH) using compromised credentials.
- **T1505.003: Server Software Component: Web Shell**
  - Threat actors use their unauthorized access to implant web shells on internal and external-facing web servers, allowing them to execute commands on compromised devices.
- **T1059.001: Command and Scripting Interpreter: PowerShell**
  - Attackers leverage code execution to execute arbitrary PowerShell commands.
- **T1203: Exploitation for Client Execution**

---

[2] "Ivanti Connect Secure [Datasheet]." *www.ivanti.com*,www.ivanti.com/resources/v/doc/ivi/2516/9c01b1c709cb.

[3] "Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways" February 29, 2024. Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways CISA.

- Threat actors can exploit a command-injection vulnerability in web components of Ivanti Connect Secure and Policy Secure, which allow an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

Mitigation Measures:

The recommended mitigating strategies below may be used by MTS entities to decrease a threat actor's opportunity for exploitation.

- **Limit outbound connections from Secure Sockets Layer (SSL) Virtual Private Network (VPN) appliances.**
  - This will limit the ability of a threat actor to download tools or malware onto the device or establish outbound connections to command and control (C2) servers.
- **Ensure SSL VPN Appliances configured with Active Directory or Lightweight Directory Access Protocol (LDAP) use low privilege accounts for the LDAP bind.**
- **Limit SSL VPN connections to unprivileged accounts.**
  - This will help limit the exposure of privileged account credentials.
- **Secure remote access tools**
  - Implement application controls, including allowlisting applications and remote access programs to block unlisted application execution and prevent installation of unauthorized remote access software.
- **Keep all operating systems, software, and firmware up to date.**
  - Ensure timely patch management to mitigate known vulnerabilities, especially on internet-facing systems.
- **Strictly regulate the use of RDP.**
  - Only enable RDP where necessary. If enabled, audit the network for systems using RDP, close unused RDP ports, log all RDP login attempts, and enforce account lockouts after a number of failed login attempts.
- **Configure the Windows Registry to require User Account Control approval for any PsExec operations.**
  - Requiring administrator privileges for PsExec operations will reduce the risk of a threat actor moving laterally using this tactic.
- **Maintain and enforce a strong password policy.**
  - Require strong passwords with a minimum of 15 characters and enforce account lockouts after multiple failed login attempts.
- **Monitor for known Indicators of Compromise (IOCs).**
  - MTS entities are encouraged to utilize the IOCs listed in Appendix A to monitor their infrastructure for potential compromises. In the event of a compromise, entities are encouraged to report their situation to the National Response Center.
- **When choosing a VPN, including deciding whether to continue operating Ivanti Connect Secure and Policy Secure Gateways, MTS entities should consider vendors who:**
  - Do not use proprietary protocols or non-standard features.
  - Provide a Software Bill of Materials to identify and enable remediation of embedded software vulnerabilities.

- Allow a restore from trusted media to establish a root of trust.
- Are a CVE Numbering Authority so that CVEs are assigned to vulnerabilities in a timely matter.
- Have clear end-of-life policies to prepare customers for updating to supported product versions.

If your organization has any questions related to this alert, please contact the U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.

Appendix A: IOCs

Ivanti Connect Secure VPN IOCs

Filename	**/home/perl/DSLogConfig.pm**
Filename	**/usr/bin/a.sh**
Filename	**/bin/netmon**
Filename	**/home/venv3/lib/python3.6/site-packages/*.egg**
Filename	**/home/etc/sql/dsserver/sessionserver.pl**
Filename	**/home/etc/sql/dsserver/sessionserver.sh**
Filename	**/home/webserver/htdocs/dana-na/auth/compcheckresult.cgi**
Filename	**/home/webserver/htdocs/dana-na/auth/lastauthserverused.js**
IPv4	**88.119.169[.]227**
IPv4	**103.13.28[.]40**
IPv4	**46.8.68[.]100**
IPv4	**206.189.208[.]156**
IPv4	**75.145.243[.]85**
IPv4	**47.207.9[.]89**
IPv4	**98.160.48[.]170**
IPv4	**173.220.106[.]166**
IPv4	**73.128.178[.]221**
IPv4	**50.243.177[.]161**
IPv4	**50.213.208[.]89**
IPv4	**64.24.179[.]210**
IPv4	**75.145.224[.]109**
IPv4	**50.215.39[.]49**
IPv4	**71.127.149[.]194**
IPv4	**173.53.43[.]7**
Hostname	**gpoaccess[.]com**
Hostname	**webb-institute[.]com**
Hostname	**symantke[.]com**

Host-Based IOCs

Domain	**symantke[.]com**
Domain	**miltonhouse[.]nl**
Domain	**entraide-internationale[.]fr**

Domain	**api.d-n-s[.]name**
Domain	**cpanel.netbar[.]org**
Domain	**clickcom[.]click**
Domain	**clicko[.]click**
Domain	**duorhytm[.]fun**
Domain	**line-api[.]com**
Domain	**areekaweb[.]com**
Domain	**ehangmun[.]com**
Domain	**secure-cama[.]com**
IPv4	**146.0.228[.]66**
IPv4	**159.65.130[.]146**
IPv4	**8.137.112[.]245**
IPv4	**91.92.254[.]14**
IPv4	**186.179.39[.]235**
IPv4	**50.215.39[.]49**
IPv4	**45.61.136[.]14**
IPv4	**173.220.106[.]166**
Hash	**ed4b855941d6d7e07aacf016a2402c4c870876a050a4a547af194f5a9b47945f**
Hash	**3045f5b3d355a9ab26ab6f44cc831a83**
Hash	**3d97f55a03ceb4f71671aa2ecf5b24e9**
Hash	**2ec505088b942c234f39a37188e80d7a**
Hash	**8eb042da6ba683ef1bae460af103cc44**
Hash	**a739bd4c2b9f3679f43579711448786f**
Hash	**a81813f70151a022ea1065b7f4d6b5ab**
Hash	**d0c7a334a4d9dcd3c6335ae13bee59ea**
Hash	**e8489983d73ed30a4240a14b1f161254**

References:

"Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN" 10 Jan. 2024. Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN | Volexity

"Cutting Edge, Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation" 2 Feb. 2024. Cutting Edge, Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation | Mandiant

"Ivanti Connect Secure [Datasheet]." *Www.ivanti.com*,www.ivanti.com/resources/v/doc/ivi/2516/9c01b1c709cb.

"KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways" 29 Feb. 2024. KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways

"Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways" 29 Feb. 2024. Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways | CISA.