Security for the greater good

Newscast

Vulnerability in Ivanti

2024-02-16 I **TLP:CLEAR** I CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

IVANTI 2

CVE-2024-21887 2

Type of vulnerability 2

Risk 2

Criticality (CVSS v3.1 base score) 3

Affected products 3

Recommendations 3

Proof of concept 3

CVE-2023-46805 4

Type of vulnerability 4

Risk 4

Criticality (CVSS v3.1 base score) 4

Affected products 4

Recommendations 5

Proof of concept 5

CVE-2024-21893 6

Type of vulnerability 6

Risk 6

Criticality (CVSS v3.1 base score) 6

Affected products 6

Recommendations 6

Proof of concept 7

Yara Rules 8

SOURCES 12

IVANTI

Ivanti published a security advisory on 10 January 2024 concerning two vulnerabilities in *Ivanti Connect Secure* (ICS) and *Ivanti Policy Secure gateways*.

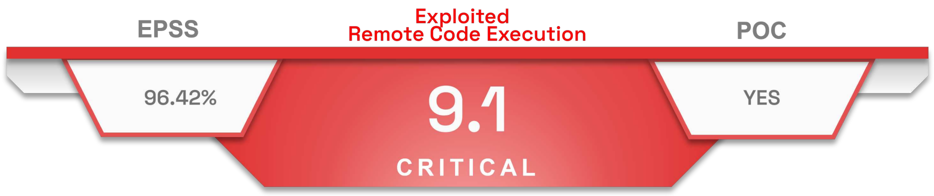
Update from 31 January 2024: Ivanti updated its advisory concerning the discovery of two new vulnerabilities (CVE-2024-21888 and CVE-2024-21893) affecting *Ivanti Neurons for ZTA*, *Ivanti Connect Secure* (ICS) and *Ivanti Policy Secure gateways*.

Update from 02 February 2024: To improve readability of the editor's recommendations, these sections have been updated.

Update from 12 February 2024: Additional Indicators of Compromise (IoCs) have been added to aid detection.

Update from 16 February 2024 : Ivanti has released new patches for Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA.

CVE-2024-21887



EPSS
96.42%
Exploited
Remote Code Execution
9.1
CRITICAL
POC
YES

A command injection vulnerability in the web components of *Ivanti Connect Secure* (CS) and *Ivanti Policy Secure* (PS) has been discovered by Volexity security researchers.

By sending a specifically crafted request, a remote and authenticated attacker can execute arbitrary code.

The CVE-2024-21887 (arbitrary code execution) can be exploited in conjunction with CVE-2023-46805 (authentication bypass).

Volexity observed the exploitation of this vulnerability and attributed it to the UTA0178 APT group.
CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on 10 January 2024.
Update from 12 January 2024: On the 11 January 2024, the CERT-FR published an alert concerning the exploitation this vulnerability.
On the same day, Mandiant published a report concerning the exploitation of these two vulnerabilities and provided additional detection rules and indicators of compromise.
Update from 22 January 2024: Ivanti has provided evidence of new exploitation of these vulnerabilities, as well as new indicators of compromise.

Update from 12 January 2024: Mandiant's advisory highlights the use of several custom malwares during and after the attacks. These malwares allow the threat actors to maintain persistence in the compromised system, avoid detection and harvest credentials.

Type of vulnerability

- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Risk

- Remote Code Execution

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	High	Impact on integrity	High
User Interaction	None	Impact on availability	High

Affected products

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

Recommendations

Update from 16 February 2024 :

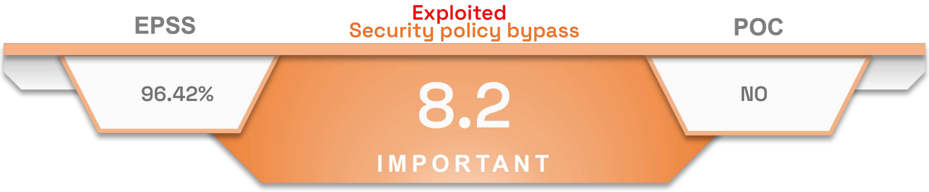
- Update Ivanti Connect Secure to the version 9.1R14.5, 9.1R15.3, 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.1R6.1, 22.3R1.1, 22.2R4.1, 22.4R1.1, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2 or later.
- Update Ivanti Policy Secure to the version 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.4R1.1, 22.5R1.2, 22.6R1.1 or later.
- Before applying the patches, Ivanti recommends ensuring the integrity of the concerned equipment with the provided *Ivanti integrity checker* (*ICT*) tool. The procedure for installing this workaround is available in their advisory.
- Ivanti also recommends resetting devices before applying the patch, to prevent attackers from maintaining persistence. As well as changing all passwords (users and administrators), API keys and renewing the certificates deployed on the equipments.
- If the patch cannot be deployed, it is necessary to implement the workaround by importing the *mitigation.release.20240107.1.xml* file via their download portal. The associated procedure is available in their KB article.
- Additional information is available in Ivanti's advisory.

Proof of concept

Update from 22 January 2024: A proof of concept is available in open source.

Update from 31 January 2024:

CVE-2023-46805



EPSS 96.42%

Exploited
Security policy bypass

8.2
IMPORTANT

POC NO

An authentication check flaw in the web components of *Ivanti Connect Secure* and *Ivanti Policy Secure* has been discovered by Volexity security researchers.

Exploitation of this vulnerability by a remote, unauthenticated attacker can bypass security controls and gain access to web service information.

> Volexity observed the exploitation of this vulnerability and attributed it to the UTA0178 APT group.
> CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on 10 January 2024.
> Update from 12 January 2024: On the 11 January 2024, the CERT-FR published an alert concerning the exploitation this vulnerability.
> On the same day, Mandiant published a report concerning the exploitation of these two vulnerabilities and provided additional detection rules and indicators of compromise.
> Update from 22 January 2024: Ivanti has provided evidence of new exploitation of these vulnerabilities, as well as new indicators of compromise.

> Update: Mandiant's advisory highlights the use of several custom malwares during and after the attacks. These malwares allow the threat actors to maintain persistence in the compromised system, avoid detection and harvest credentials.

Type of vulnerability

- **CWE-287** : Improper Authentication

Risk

- Bypass security policy

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	Low
User Interaction	None	Impact on availability	None

Affected products

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

Recommendations

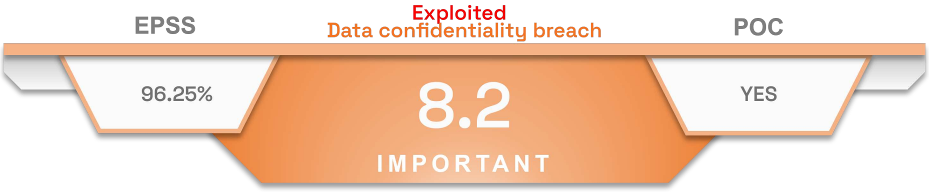
Update from 16 February 2024 :

- Update Ivanti Connect Secure to the version 9.1R14.5, 9.1R15.3, 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.1R6.1, 22.3R1.1, 22.2R4.1, 22.4R1.1, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2 or later.
- Update Ivanti Policy Secure to the version 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.4R1.1, 22.5R1.2, 22.6R1.1 or later.
- Before applying the patches, Ivanti recommends ensuring the integrity of the concerned equipment with the provided *Ivanti integrity checker* (*ICT*) tool. The procedure for installing this workaround is available in their advisory.
- Ivanti also recommends resetting devices before applying the patch, to prevent attackers from maintaining persistence. As well as changing all passwords (users and administrators), API keys and renewing the certificates deployed on the equipments.
- If the patch cannot be deployed, it is necessary to implement the workaround by importing the *mitigation.release.20240107.1.xml* file via their download portal. The associated procedure is available in their KB article.
- Additional information is available in Ivanti's advisory.

Proof of concept

Update from 22 January 2024: A proof of concept is available in open source.

CVE-2024-21893



A Server-Side Request Forgery vulnerability in Ivanti's SAML component allows an unauthenticated attacker, by sending specially crafted requests, to access restricted data.

This vulnerability is exploited.

Type of vulnerability

- **CWE-918**: Server-Side Request Forgery (SSRF)

Risk

- Data confidentiality breach

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	Low
User Interaction	None	Impact on availability	None

Affected products

- Ivanti Connect Secure and Ivanti Policy Secure versions 9.x and 22.x
- Ivanti Neurons for ZTA

Recommendations

Update from 16 February 2024 :

- Update Ivanti Connect Secure to the version 9.1R14.5, 9.1R15.3, 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.1R6.1, 22.3R1.1, 22.2R4.1, 22.4R1.1, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2 or later.
- Update Ivanti Policy Secure to the version 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.4R1.1, 22.5R1.2, 22.6R1.1 or later.
- Update ZTA gateways to version 22.5R1.6, 22.6R1.5, 22.6R1.7 or later.
- Before applying the patches, Ivanti recommends ensuring the integrity of the concerned equipment with the provided *Ivanti integrity checker* (*ICT*) tool. The procedure for installing this workaround is available in their advisory.
- Ivanti also recommends resetting devices before applying the patch, to prevent attackers from maintaining persistence. As well as changing all passwords (users and administrators), API keys and renewing the certificates deployed on the equipments.
- If the patch cannot be deployed, it is necessary to implement the workaround by importing the *mitigation.release.20240107.1.xml* file via their download portal. The associated procedure is available in their KB article.
- Additional information is available in Ivanti's advisory.

Proof of concept

Update from 12 February 2024: A proof of concept is available in open source.

Yara Rules

ZIPLINE Backdoor

```
rule M_Hunting_Backdoor_ZIPLINE_1 {
  meta:
    author = "Mandiant"
    description = "This rule detects unique strings in ZIPLINE, a passive ELF backdoor that waits for
incoming TCP connections to receive commands from the threat actor."
  strings:
    $s1 = "SSH-2.0-OpenSSH_0.3xx" ascii
    $s2 = "$(exec $installer $@)" ascii
    $t1 = "./installer/do-install" ascii
    $t2 = "./installer/bom_files/" ascii
    $t3 = "/tmp/data/root/etc/ld.so.preload" ascii
    $t4 = "/tmp/data/root/home/etc/manifest/exclusion_list" ascii
  condition:
    uint32(0) == 0x464c457f and
    filesize < 5MB and
    ((1 of ($s*)) or
    (3 of ($t*)))
}
```

WIREFIRE Dropper

```
rule M_Hunting_Dropper_WIREFIRE_1 {
  meta:
    author = "Mandiant"
    description = "This rule detects WIREFIRE, a web shell written in Python that exists as trojanized logic
to a component of the pulse secure appliance."
    md5 = "6de651357a15efd01db4e658249d4981"
  strings:
    $s1 = "zlib.decompress(aes.decrypt(base64.b64decode(" ascii
    $s2 = "aes.encrypt(t+('\\x00'*(16-len(t)%16))" ascii
    $s3 = "Handles DELETE request to delete an existing visits data." ascii
    $s4 = "request.data.decode().startswith('GIF'):" ascii
    $s5 = "Utils.api_log_admin" ascii
  condition:
    filesize < 10KB
    and all of them
}
```

Aditional YARA rules are available in Mandiant and Volexity advisories.

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	Domain	gpoaccess[.]com	Suspected UTA0178 domain discovered via domain registration patterns
TLP:CLEAR	Domain	webb-institute[.]com	Suspected UTA0178 domain discovered via domain registration patterns
TLP:CLEAR	Domain	symantke[.]com	WARPWIRE C2 server
TLP:CLEAR	Domain	miltonhouse[.]nl	WARPWIRE C2 server
TLP:CLEAR	Domain	entraide-internationale[.]fr	WARPWIRE C2 server
TLP:CLEAR	Domain	api.d-n-s[.]name	WARPWIRE variant C2 server
TLP:CLEAR	Domain	cpanel.netbar[.]org	WARPWIRE variant C2 server
TLP:CLEAR	Domain	clickcom[.]click	WARPWIRE variant C2 server
TLP:CLEAR	Domain	clicko[.]click	WARPWIRE variant C2 server
TLP:CLEAR	Domain	duorhytm[.]fun	WARPWIRE variant C2 server
TLP:CLEAR	Domain	line-api[.]com	WARPWIRE variant C2 server
TLP:CLEAR	Domain	areekaweb[.]com	WARPWIRE variant C2 server
TLP:CLEAR	Domain	ehangmun[.]com	WARPWIRE variant C2 server
TLP:CLEAR	Domain	secure-cama[.]com	WARPWIRE variant C2 server
TLP:CLEAR	URL	103.233.11[.]5:1999/doc	URL used to download Payloads
TLP:CLEAR	URL	45.130.22[.]219/ivanti.js	URL used to download Payloads
TLP:CLEAR	URL	45.130.22[.]219/ivanti	URL used to download Payloads
TLP:CLEAR	URL	137.220.130[.]2/doc	URL used to download Payloads
TLP:CLEAR	URL	124.156.132[.]142:6999/python	URL used to download Payloads
TLP:CLEAR	URL	raw.githubusercontent[.]com/momika233/test/main/m.sh	URL used to download Payloads
TLP:CLEAR	URL	github[.]com/momika233/test/raw/main/watchbog	URL used to download watchbog
TLP:CLEAR	URL	github[.]com/momika233/test/raw/main/watchd0g	URL used to download watchd0g
TLP:CLEAR	IP	206.189.208[.]156	DigitalOcean IP address tied to UTA0178 (Hosting service so false positive risk)
TLP:CLEAR	IP	75.145.243[.]85	UTA0178 IP address observed interacting with compromised device
TLP:CLEAR	IP	47.207.9[.]89	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	98.160.48[.]170	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	173.220.106[.]166	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	73.128.178[.]221	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	50.243.177[.]161	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	50.213.208[.]89	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	IP	64.24.179[.]210	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	75.145.224[.]109	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	50.215.39[.]49	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	71.127.149[.]194	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	173.53.43[.]7	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
TLP:CLEAR	IP	146.0.228[.]66	WARPWIRE variant C2 server
TLP:CLEAR	IP	159.65.130[.]146	WARPWIRE variant C2 server (Hosting service so false positive risk)
TLP:CLEAR	IP	8.137.112[.]245	WARPWIRE variant C2 server (Hosting service so false positive risk)
TLP:CLEAR	IP	91.92.254[.]14	WARPWIRE variant C2 server
TLP:CLEAR	IP	186.179.39[.]235	Mass exploitation activity
TLP:CLEAR	IP	45.61.136[.]14	Post-exploitation activity
TLP:CLEAR	IP	138.68.61[.]82	IPs contacted to download Payloads (Hosting service so false positive risk)
TLP:CLEAR	IP	192.252.183[.]116	IPs contacted to download Payloads
TLP:CLEAR	IP	141.98.7[.]6	IPs contacted to download Payloads (Hosting service so false positive risk)
TLP:CLEAR	IP	103.215.77[.]51	IPs contacted to download Payloads
TLP:CLEAR	IP	45.152.66[.]151	IPs contacted to download Payloads (Hosting service so false positive risk)
TLP:CLEAR	MD5 I Filename	3045f5b3d355a9ab26ab6f44cc831a83 I health.py	CHAINLINE Web Shell
TLP:CLEAR	MD5 I Filename	3d97f55a03ceb4f71671aa2ecf5b24e9 I compcheckresult.cgi	LIGHTWIRE Web Shell
TLP:CLEAR	MD5 I Filename	2ec505088b942c234f39a37188e80d7a I lastauthserverused.js	WARPWIRE Credential harvester
TLP:CLEAR	MD5 I Filename	8eb042da6ba683ef1bae460af103cc44 I lastauthserverused.js	WARPWIRE Credential harvester
TLP:CLEAR	MD5 I Filename	a739bd4c2b9f3679f43579711448786f I lastauthserverused.js	WARPWIRE Credential harvester
TLP:CLEAR	MD5 I Filename	a81813f70151a022ea1065b7f4d6b5ab I lastauthserverused.js	WARPWIRE Credential harvester
TLP:CLEAR	MD5 I Filename	d0c7a334a4d9dcd3c6335ae13bee59ea I lastauthserverused.js	WARPWIRE Credential harvester
TLP:CLEAR	MD5 I Filename	e8489983d73ed30a4240a14b1f161254 I lastauthserverused.js	WARPWIRE Credential harvester
TLP:CLEAR	MD5 I Filename	465600cece80861497e8c1c86a07a23e I category.py	FRAMESTING Web Shell
TLP:CLEAR	MD5 I Filename	65f19b39dc43f202a6d26223d0472b66 I watchd0g	Backdoor KrustyLoader written in Go

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	SHA1 | Filename	46e0847be3dab555790446f267e2c2aea5a3b9bb | watchd0g	Backdoor KrustyLoader written in Go
TLP:CLEAR	SHA256 | Filename	1e1e94bd2bfd5054265123bf55c4cf6ce87de6692d9329bda4a37e89272356e4 | watchd0g	Backdoor KrustyLoader written in Go
TLP:CLEAR	MD5 | Filename	03356c7fac38d09b0d07873f0d3f2b37 | watchbog	Watchbog malware written in Go
TLP:CLEAR	SHA1 | Filename	2a76d2d4bef67d565c331fc6945724d31bdf989c | watchbog	Watchbog malware written in Go
TLP:CLEAR	SHA256 | Filename	8eadb5beeb21d4a95dacd133cb2b934342fcb39fe4df2a8387a0d5499c72450d | watchbog	Watchbog malware written in Go
TLP:CLEAR	SHA256 | Filename	cf20940907be484440e8343aa05505ad2e4d6d1f24ef29504bfa54ade4a8455f | m.sh	Watchbog and watchd0g dropper
TLP:CLEAR	Filename	visits.py	WIREFIRE Web Shell
TLP:CLEAR	Filename	sessionserver.sh	THINSPOOL Web Shell dropper
TLP:CLEAR	Filename	sessionserver.pl	THINSPOOL Utility Script
TLP:CLEAR	Filename	libsecure.so.1	ZIPLINE Passive backdoor

Sources

Ivanti

- 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?language=en_US
- https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
- https://www.cisa.gov/news-events/alerts/2024/01/10/ivanti-releases-security-update-connect-secure-and-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.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day
- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-001/
- https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US
- https://www.cisa.gov/news-events/alerts/2024/01/19/cisa-issues-emergency-directive-ivanti-vulnerabilities
- https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation
- https://unit42.paloaltonetworks.com/threat-brief-ivanti-cve-2023-46805-cve-2024-21887/
- https://www.greynoise.io/blog/ivanti-connect-secure-exploited-to-install-cryptominers

CVE-2024-21887

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21887

CVE-2023-46805

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46805

CVE-2024-21893

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21893