

Intelligence Report

Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways

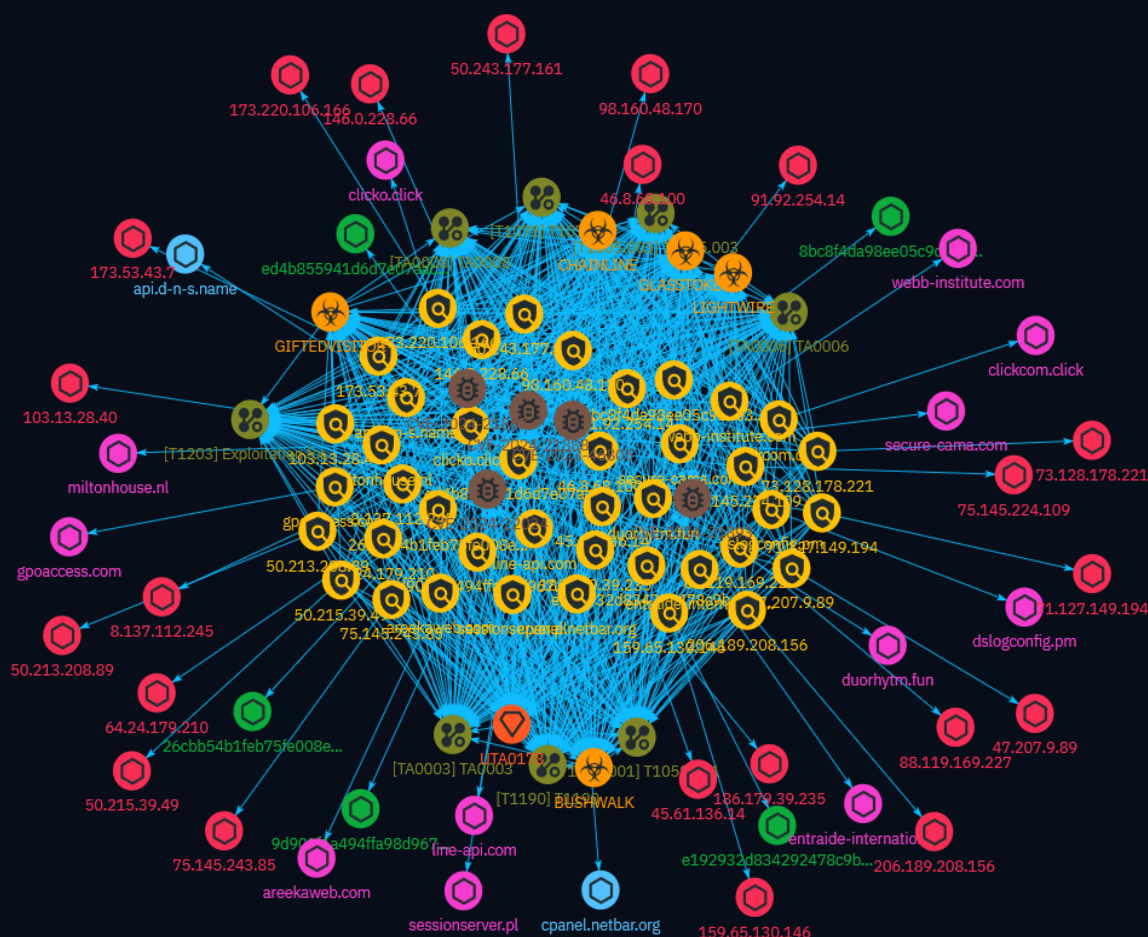


Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Indicator	6
● Malware	30
● Vulnerability	31
● Intrusion-Set	33
● Attack-Pattern	34

Observables

● StixFile	39
● IPv4-Addr	40

●	Domain-Name	42
---	-------------	----

●	Hostname	43
---	----------	----

External References

●	External References	44
---	---------------------	----

Overview

Description

Cyber threat actors are actively exploiting multiple vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways that can be chained to bypass authentication, craft malicious requests, and execute arbitrary commands. This enables threat actors to implant web shells for persistence and harvest credentials stored on compromised devices.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

ed4b855941d6d7e07aacf016a2402c4c870876a050a4a547af194f5a9b47945f

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'ed4b855941d6d7e07aacf016a2402c4c870876a050a4a547af194f5a9b47945f']

Name

e192932d834292478c9b1032543c53edfc2b252fdf7e27e4c438f4b249544eeb

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'e192932d834292478c9b1032543c53edfc2b252fdf7e27e4c438f4b249544eeb']

Name

8bc8f4da98ee05c9d403d2cb76097818de0b524d90bea8ed846615e42cb031d2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'8bc8f4da98ee05c9d403d2cb76097818de0b524d90bea8ed846615e42cb031d2']

Name

9d901f1a494ffa98d967ee6ee30a46402c12a807ce425d5f51252eb69941d988

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'9d901f1a494ffa98d967ee6ee30a46402c12a807ce425d5f51252eb69941d988']

Name

26cbb54b1feb75fe008e36285334d747428f80aacdb57badf294e597f3e9430d

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'26cbb54b1feb75fe008e36285334d747428f80aacdb57badf294e597f3e9430d']

Name

46.8.68.100

Description

- **Zip Code:** N/A - **ISP:** LLC Gazpromneft ITO - **ASN:** 56669 - **Organization:** LLC Gazpromneft ITO - **Is Crawler:** False - **Timezone:** Europe/Moscow - **Mobile:** False - **Host:** 46.8.68.100 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RU - **Region:** St.-Petersburg - **City:** St Petersburg - **Latitude:** 59.94169998 - **Longitude:** 30.30960083

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.8.68.100']

Name

88.119.169.227

Description

ISP: Informacines sistemas ir technologijos, UAB **OS:** Windows (build 10.0.17763)
----- Services: **3389:** Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00 Remote
Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version
1809) OS Build: 10.0.17763 Target Name: WIN-R4ANN5H1BDJ NetBIOS Domain Name: WIN-

R4ANN5H1BDJ NetBIOS Computer Name: WIN-R4ANN5H1BDJ DNS Domain Name: WIN-R4ANN5H1BDJ FQDN: WIN-R4ANN5H1BDJ ~~~ -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.119.169.227']

Name

103.13.28.40

Description

ISP: Siamdata Communication Co.,Ltd. **OS:** - ----- Services:
53: ~~~ ~~~ -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.13.28.40']

Name

45.61.136.14

Description

Post-exploitation activity

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.61.136.14']

Name

186.179.39.235

Description

Mass exploitation activity

Pattern Type

stix

Pattern

[ipv4-addr:value = '186.179.39.235']

Name

8.137.112.245

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[ipv4-addr:value = '8.137.112.245']

Name

159.65.130.146

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.65.130.146']

Name

146.0.228.66

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.0.228.66']

Name

secure-cama.com

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[domain-name:value = 'secure-cama.com']

Name

areekaweb.com

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[domain-name:value = 'areekaweb.com']

Name

line-api.com

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[domain-name:value = 'line-api.com']

Name

duorhytm.fun

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[domain-name:value = 'duorhytm.fun']

Name

clicko.click

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[domain-name:value = 'clicko.click']

Name

clickcom.click

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[domain-name:value = 'clickcom.click']

Name

cpanel.netbar.org

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

```
[hostname:value = 'cpanel.netbar.org']
```

Name

```
api.d-n-s.name
```

Description

WARPWIRE variant C2 server

Pattern Type

```
stix
```

Pattern

```
[hostname:value = 'api.d-n-s.name']
```

Name

```
entraide-internationale.fr
```

Description

WARPWIRE variant C2 server

Pattern Type

```
stix
```

Pattern

```
[domain-name:value = 'entraide-internationale.fr']
```

Name

miltonhouse.nl

Description

WARPWIRE variant C2 server

Pattern Type

stix

Pattern

[domain-name:value = 'miltonhouse.nl']

Name

91.92.254.14

Description

Malicious SSL connections

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.92.254.14']

Name

dslogconfig.pm

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'just now', 'timestamp': 1704967518, 'iso': '2024-01-11T05:05:18-05:00'} - **IPQS: Domain:** dslogconfig.pm - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'dslogconfig.pm']

Name

gpoaccess.com

Description

Suspected UTA0178 domain discovered via domain registration patterns

Pattern Type

stix

Pattern

[domain-name:value = 'gpoaccess.com']

Name

webb-institute.com

Description
Suspected UTA0178 domain discovered via domain registration patterns
Pattern Type
stix
Pattern
[domain-name:value = 'webb-institute.com']
Name
sessionserver.pl
Pattern Type
stix
Pattern
[domain-name:value = 'sessionserver.pl']
Name
173.53.43.7
Description
<pre>**ISP:** Verizon Business **OS:** None ----- Hostnames: - static-173-53-43-7.rcmdva.fios.verizon.net ----- Domains: - verizon.net ----- Services: **80:** ~~~ HTTP/1.1 200 OK Content-Type: text/html Accept-Ranges: bytes ETag: "-1176448012" Last-Modified: Sun, 09 Jul 2023 10:14:53 GMT Content-Length: 500 Date: Wed, 10 Jan 2024 21:38:39 GMT Server: lighttpd ~~~ ----- **444:** ~~~ ~~~ ----- **500:** ~~~ VPN (IKE) Initiator SPI: 7068357663706138</pre>

Responder SPI: 687a706b62663364 Next Payload: Notification (N) Version: 1.0 Exchange Type: Informational Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length: 40 ~~~ -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.53.43.7']

Name

71.127.149.194

Description

****ISP:**** Verizon Business ****OS:**** None ----- Hostnames: -
mail.atslink.com ----- Domains: - atslink.com -----
Services: **22:** ~~~ SSH-2.0-XXXX Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAQCKs+wiVy5mwX/
5pDvaa5NpHDonmIKyNY7ShPREkMBqVv1 OwMmlvJeFmW1Af7zSDNkdKqv4l/
kZ8ToftStz6jAmYwmy1bTfbB8TRhNSEKDa72ULQUWKuIFlhZE
wl2iMJ9EgAiDJj4shoXUMhmQ1GOoMsPQRtmjg4ybP4ylPEQsRZ04GpXD2JBYTHuCyV8wcvRSg/VT
b076McAku1G3EKJecmqm9CIQNYCZvqYuOlwqt/2k3k/zz+lavWGmTYK/
FeZgwCKBZYE2cWcT5Xb G9aGMUuO7X8cYYd8/h1vQhdYRRQxynBptd42xaMXbOEX3Kxoaal/
yUQM3IDO8CgMcmKp Fingerprint: 5a:f5:df:46:a0:a5:09:80:9e:19:03:49:c5:ae:42:23 Kex
Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-
sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1
kexguess2@matt.ucc.asn.au Server Host Key Algorithms: ssh-rsa ssh-dss Encryption
Algorithms: aes128-ctr aes256-ctr aes128-cbc aes256-cbc twofish256-cbc twofish-cbc
twofish128-cbc 3des-ctr 3des-cbc MAC Algorithms: hmac-sha1-96 hmac-sha1 hmac-sha2-256
hmac-sha2-512 hmac-md5 Compression Algorithms: zlib@openssh.com none ~~~
----- ****500:**** ~~~ VPN (IKE) Initiator SPI: 346f35686b336434 Responder SPI:
7161737967663879 Next Payload: Notification (N) Version: 1.0 Exchange Type: Informational
Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length:
40 ~~~ ----- ****4443:**** ~~~ HTTP/1.1 200 OK Date: Mon, 08 Jan 2024 21:12:42 GMT
Server: xxxx X-Frame-Options: SAMEORIGIN Content-Type: text/html; charset=UTF-8 Expires:
Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-cache Pragma: no-cache Content-Length:

```
6445 Vary: Accept-Encoding Set-Cookie: JSESSIONID=p3u57ucd0utfaq85obu4lo29;Path=/
corporate;HttpOnly;Secure ~~~ HEARTBLEED: 2024/01/08 21:12:51 71.127.149.194:4443 - SAFE
----- **8090:** ~~~ ----- **8443:** ~~~ HTTP/1.1 200 OK Date: Wed, 27
Dec 2023 11:51:40 GMT Server: xxxx X-Frame-Options: SAMEORIGIN Content-Type: text/html;
charset=UTF-8 Expires: Thu, 01 Jan 1970 00:00:00 GMT Content-Length: 6441 Set-Cookie:
JSESSIONID=1ujx5bbrw7g3it84fyoonzmz0;Path=/corporate;HttpOnly;Secure Connection:
close ~~~ HEARTBLEED: 2023/12/27 11:51:47 71.127.149.194:8443 - SAFE -----
```

Pattern Type

stix

Pattern

[ipv4-addr:value = '71.127.149.194']

Name

64.24.179.210

Description

```
**ISP:** Windstream Communications LLC **OS:** None -----
Hostnames: ----- Domains: ----- Services: **8443:**
~~~ HTTP/1.1 200 OK Date: Mon, 01 Jan 2024 11:18:46 GMT Server: xxxx X-Frame-Options:
SAMEORIGIN Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff
Content-Security-Policy: default-src http: https: data: ws: wss: blob: 'unsafe-inline' 'unsafe-
eval'; worker-src 'self' blob: X-XSS-Protection: 1; mode=block Content-Type: text/html;
charset=UTF-8 Expires: Thu, 01 Jan 1970 00:00:00 GMT Content-Length: 6441 Set-Cookie:
JSESSIONID=1tddjenmo7v6g14dlbzdmgunk;Path=/corporate;HttpOnly;Secure Connection:
close ~~~ HEARTBLEED: 2024/01/01 11:18:58 64.24.179.210:8443 - SAFE -----
```

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.24.179.210']

Name

50.243.177.161

Description

ISP: Comcast Cable Communications, LLC **OS:** None -----
 Hostnames: - 50-243-177-161-static.hfc.comcastbusiness.net -----
 Domains: - comcastbusiness.net ----- Services: **443:** HTTP/1.1 200
 OK Date: Mon, 08 Jan 2024 08:17:42 GMT Content-Type: text/html; charset=UTF-8 Expires:
 Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-cache Pragma: no-cache Content-Length:
 6332 Set-Cookie: JSESSIONID=hdes5o9m4epc1t8pfuivnkxb; Path=/corporate Vary: Accept-
 Encoding HEARTBLEED: 2024/01/08 08:17:55 50.243.177.161:443 - SAFE -----
 500: VPN (IKE) Initiator SPI: 6c747570366c3236 Responder SPI: 366c6a656e76626c Next
 Payload: Notification (N) Version: 1.0 Exchange Type: Informational Flags: Encryption: False
 Commit: False Authentication: False Message ID: 00000000 Length: 40 -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.243.177.161']

Name

75.145.224.109

Description

ISP: Comcast Cable Communications, LLC **OS:** None -----
 Hostnames: - 75-145-224-109-Miami.hfc.comcastbusiness.net -----
 Domains: - comcastbusiness.net ----- Services: **53:** Recursion:
 enabled ----- **500:** VPN (IKE) Initiator SPI: 3532746435786c72 Responder
 SPI: 7636613875786531 Next Payload: Notification (N) Version: 1.0 Exchange Type:

Informational Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length: 40 ~~~ ----- **5060:** ~~~ SIP/2.0 403 Forbidden Via: SIP/2.0/UDP nm;received=224.240.148.96;branch=foo;rport=26810 From: ;tag=root To: ;tag=Mitel-5000 _3915482006-905 Call-ID: 50000 CSeq: 42 OPTIONS Content-Length: 0 ~~~ ----- **8080:** ~~~ ~~~ ----- **8443:** ~~~ HTTP/1.1 200 OK Date: Wed, 10 Jan 2024 11:06:55 GMT Server: xxxx X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff Content-Security-Policy: default-src http: https: data: ws: wss: blob: 'unsafe-inline' 'unsafe-eval'; worker-src 'self' blob: X-XSS-Protection: 1; mode=block Content-Type: text/html; charset=UTF-8 Expires: Thu, 01 Jan 1970 00:00:00 GMT Content-Length: 6441 Set-Cookie: JSESSIONID=1g1o0aijlwvq31hq6r9o56p0ws;Path=/corporate;HttpOnly;Secure Connection: close ~~~ HEARTBLEED: 2024/01/10 09:47:25 75.145.224.109:8443 - SAFE -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '75.145.224.109']

Name

50.215.39.49

Description

ISP: Comcast Cable Communications, LLC **OS:** None -----
Hostnames: ----- Domains: ----- Services: **443:** ~~~
HTTP/1.1 200 OK Date: Thu, 11 Jan 2024 02:13:22 GMT X-Frame-Options: SAMEORIGIN Content-Type: text/html; charset=UTF-8 Expires: Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-cache Pragma: no-cache Content-Length: 6445 Set-Cookie: JSESSIONID=17tnxafo9f8bwf9adcqzf3tgl;Path=/corporate;HttpOnly;Secure Vary: Accept-Encoding ~~~ HEARTBLEED: 2024/01/11 02:13:38 50.215.39.49:443 - SAFE -----
500: ~~~ VPN (IKE) Initiator SPI: 796f793779356d30 Responder SPI: 6e35656c78756266 Next Payload: Notification (N) Version: 1.0 Exchange Type: Informational Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length: 40 ~~~ -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.215.39.49']

Name

73.128.178.221

Description

****ISP:**** Comcast Cable Communications, LLC ****OS:**** None -----
 Hostnames: - c-73-128-178-221.hsd1.md.comcast.net ----- Domains: -
 comcast.net ----- Services: ****22:**** ~~~ SSH-2.0-XXXX Key type: ssh-rsa Key:
 AAAAB3NzaC1yc2EAAAADAQABAAQAgXPHgULMdoHD+/
 t2maLTseWSMmXRtSyLZs7pA6stFGV3b7j id9JVLLAnCd6GcAOpNYM01Ia/TKZGb/
 XUsrKuD7yT3+LrR/1q3onOjq7q+p50xU33Fa+dwYSo3m5 7i5tszFQbKbe6NQgYMA/
 mAzj25CiB05xTgrbE9/B3zR48Tj3V8c= Fingerprint: 57:94:42:63:a1:91:0b:58:a6:33:cb:db:fe:b5:83:38
 Kex Algorithms: diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss
 Encryption Algorithms: aes128-ctr 3des-ctr aes256-ctr aes128-cbc 3des-cbc aes256-cbc
 twofish256-cbc twofish-cbc twofish128-cbc blowfish-cbc MAC Algorithms: hmac-sha1-96
 hmac-sha1 hmac-md5 Compression Algorithms: zlib zlib@openssh.com none ~~~
 ----- ****443:**** ~~~ HTTP/1.1 200 OK Date: Thu, 28 Dec 2023 07:06:05 GMT Content-
 Type: text/html; charset=UTF-8 Expires: Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-
 cache Pragma: no-cache Content-Length: 6332 Set-Cookie: JSESSIONID=1tyhri19vsf56; Path=/
 corporate Vary: Accept-Encoding ~~~ HEARTBLEED: 2023/12/28 07:06:41 73.128.178.221:443 -
 SAFE -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '73.128.178.221']

Name

75.145.243.85

Description

****ISP:**** Comcast Cable Communications, LLC ****OS:**** None -----
 Hostnames: - 75-145-243-85-richmond-va.hfc.comcastbusiness.net -----
 Domains: - comcastbusiness.net ----- **Services:** ****80:**** HTTP/1.1 200
 OK Content-Type: text/html Accept-Ranges: bytes ETag: "-1422659619" Last-Modified: Fri, 08
 Sep 2023 02:59:41 GMT Content-Length: 500 Date: Fri, 29 Dec 2023 10:36:58 GMT Server:
 lighttpd ****444:**** HTTP/1.1 200 OK Date: Thu, 04 Jan 2024 11:18:30 GMT
 Server: xxxx X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=31536000 X-
 Content-Type-Options: nosniff Content-Security-Policy: default-src http: https: data: ws:
 wss: blob: 'unsafe-inline' 'unsafe-eval'; worker-src 'self' blob: X-XSS-Protection: 1;
 mode=block Content-Type: text/html; charset=UTF-8 Expires: Wed, 31 Dec 1969 00:00:00 GMT
 Cache-Control: no-cache Pragma: no-cache Content-Length: 6362 Vary: Accept-Encoding
 Set-Cookie: JSESSIONID=1scf352lv6vpd1dr168epwiwlh; Path=/corporate; HttpOnly; Secure
 HEARTBLEED: 2024/01/04 11:18:39 75.145.243.85:444 - SAFE ----- ****500:**** VPN
 (IKE) Initiator SPI: 6e343079377a7562 Responder SPI: 7a7a716e6c377030 Next Payload:
 Notification (N) Version: 1.0 Exchange Type: Informational Flags: Encryption: False Commit:
 False Authentication: False Message ID: 00000000 Length: 40 -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '75.145.243.85']

Name

173.220.106.166

Description

ISP: Cablevision Systems Corp. **OS:** None ----- Hostnames: - ool-addc6aa6.static.optonline.net ----- Domains: - optonline.net
----- Services: **22:** ~ SSH-2.0-XXXX Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAQABe7INntyM2SqHAO1BlvV+KnxRA4yA7I2/uUeF6DJZNtD
8A0VLcN3pwJURNE03caxcfqmtYW+NEksKnKYbJTL5oMZxG8s2okz579YYI97n18rp9C+h+cB7vau
VdTsBNdfpeW3sOYC4m/g0gbOEsGJnuJBCYEy2mL0o2fpj/d90FT3MqjaK3MhQsof2+Cq/5MD4r1J
PFOta8AtgZkoG0hJi685AKv8ks4nnrd03JGEHWU6li4qWqlfbwBq/Vt7wo3xcf7ojyDxt2VJKk7n
Al1jFG5uCjH/B7Fb5qCEDxMWsB+wKvwKHSTnHdl8XV9kZ5/q2J3mNbO/VhZfm2pckPeb
Fingerprint: 60:30:6b:54:4f:50:41:42:ac:a9:95:a3:a2:11:bc:f2 Kex Algorithms: curve25519-
sha256@libssh.org ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-
hellman-group14-sha1 diffie-hellman-group1-sha1 kexguess2@matt.ucc.asn.au Server Host
Key Algorithms: ssh-rsa ssh-dss Encryption Algorithms: aes128-ctr aes256-ctr aes128-cbc
aes256-cbc twofish256-cbc twofish-cbc twofish128-cbc 3des-ctr 3des-cbc MAC Algorithms:
hmac-sha1-96 hmac-sha1 hmac-sha2-256 hmac-sha2-512 hmac-md5 Compression
Algorithms: zlib@openssh.com none ~ ----- **443:** ~ HTTP/1.1 200 OK Date:
Sat, 06 Jan 2024 07:02:50 GMT Server: xxxx X-Frame-Options: SAMEORIGIN Content-Type:
text/html; charset=UTF-8 Expires: Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-cache
Pragma: no-cache Content-Length: 6362 Vary: Accept-Encoding Set-Cookie:
JSESSIONID=1m95rdm8zjoml1ohp18cl1ymut; Path=/corporate; HttpOnly; Secure ~
HEARTBLEED: 2024/01/05 13:46:40 173.220.106.166:443 - SAFE ----- **500:** ~ VPN
(IKE) Initiator SPI: 6668697069386378 Responder SPI: 37376a7979366c62 Next Payload:
Notification (N) Version: 1.0 Exchange Type: Informational Flags: Encryption: False Commit:
False Authentication: False Message ID: 00000000 Length: 40 ~ ----- **8443:**
~ HTTP/1.1 200 OK Date: Wed, 27 Dec 2023 14:19:10 GMT Server: xxxx X-Frame-Options:
SAMEORIGIN Content-Type: text/html; charset=UTF-8 Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Length: 6441 Set-Cookie: JSESSIONID=1sj1awyc43ruc14bje7262uq41; Path=/
corporate; HttpOnly; Secure Connection: close ~ HEARTBLEED: 2023/12/26 21:02:29
173.220.106.166:8443 - SAFE -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.220.106.166']

Name

47.207.9.89

Description

ISP: Frontier Communications of America, Inc. **OS:** None -----
 Hostnames: ----- Domains: ----- Services: **9443:** ~~~
 HTTP/1.1 200 OK Date: Wed, 03 Jan 2024 01:09:52 GMT Server: xxxx X-Frame-Options:
 SAMEORIGIN Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff
 Content-Security-Policy: default-src http: https: data: ws: wss: blob: 'unsafe-inline' 'unsafe-
 eval'; worker-src 'self' blob: X-XSS-Protection: 1; mode=block Content-Type: text/
 html; charset=UTF-8 Expires: Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-cache
 Pragma: no-cache Content-Length: 6445 Vary: Accept-Encoding Set-Cookie:
 JSESSIONID=if06jt2wavwubctynfdru9ne; Path=/corporate; HttpOnly; Secure ~~~ HEARTBLEED:
 2024/01/03 01:10:01 47.207.9.89:9443 - SAFE -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.207.9.89']

Name

50.213.208.89

Description

ISP: Comcast Cable Communications, LLC **OS:** None -----
 Hostnames: - 50-213-208-89-static.hfc.comcastbusiness.net -----
 Domains: - comcastbusiness.net ----- Services: **22:** ~~~ SSH-2.0-XXXX
 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAQCKs+wiVy5mwX/
 5pDvaa5NpHDonmIKyNY7ShPREkMBqVv1 OwMmlvJeFmW1Af7zSDNkdKqv4l/
 kZ8ToFTStz6jAmYwmy1bTfbB8TRhNSEKDa72ULQUWKuIFlhZE
 wl2iMJ9EgAiDJj4shoXUMhmQ1GOoMsPQRtmjg4ybP4ylPEQsRZ04GpXD2JBYTHuCyV8wcvRSg/VT
 b076McAku1G3EKJecmqm9CIQNYCZvqYuOlewqt/2k3k/zz+lavWGmTYK/
 FeZgwCKBZYE2cWcT5Xb G9aGMUuO7X8cYYd8/h1vQhdYRRQxynBptd42xaMXbOEX3Kxoa1/
 yUQM3IDO8CgMcmKp Fingerprint: 5a:f5:df:46:a0:a5:09:80:9e:19:03:49:c5:ae:42:23 Kex
 Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-
 sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1

kexguess2@matt.ucc.asn.au Server Host Key Algorithms: ssh-rsa ssh-dss Encryption Algorithms: aes128-ctr aes256-ctr aes128-cbc aes256-cbc twofish256-cbc twofish-cbc twofish128-cbc 3des-ctr 3des-cbc MAC Algorithms: hmac-sha1-96 hmac-sha1 hmac-sha2-256 hmac-sha2-512 hmac-md5 Compression Algorithms: zlib@openssh.com none ~~~
----- **80:** ~~~ HTTP/1.1 200 OK Date: Thu, 11 Jan 2024 03:34:33 GMT Server: xxxx
X-Frame-Options: SAMEORIGIN Content-Type: text/html; charset=UTF-8 Expires: Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-cache Pragma: no-cache Content-Length: 6445 Set-Cookie: JSESSIONID=1g0yryrkcpkv9132qa6my4g06v; Path=/corporate Vary: Accept-Encoding ~~~
----- **500:** ~~~ VPN (IKE) Initiator SPI: 6b6a386338697579 Responder SPI: 65666978626c796d Next Payload: Notification (N) Version: 1.0 Exchange Type: Informational
Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length: 40 ~~~
----- **4443:** ~~~ HTTP/1.1 200 OK Date: Fri, 05 Jan 2024 19:45:33 GMT
Server: xxxx X-Frame-Options: SAMEORIGIN Content-Type: text/html; charset=UTF-8 Expires: Wed, 31 Dec 1969 00:00:00 GMT Cache-Control: no-cache Pragma: no-cache Content-Length: 6445 Vary: Accept-Encoding Set-Cookie: JSESSIONID=1sn3ceg8ghpkj1xx2y5fns6cdv; Path=/corporate; HttpOnly; Secure ~~~ HEARTBLEED: 2024/01/05 19:45:40 50.213.208.89:4443 - SAFE
----- **8090:** ~~~ ----- **8443:** ~~~ HTTP/1.1 200 OK Date: Wed, 10 Jan 2024 00:02:59 GMT Server: xxxx X-Frame-Options: SAMEORIGIN Content-Type: text/html; charset=UTF-8 Expires: Thu, 01 Jan 1970 00:00:00 GMT Content-Length: 6441 Set-Cookie: JSESSIONID=p14pfubxy561jvqyh0w1f5cm; Path=/corporate; HttpOnly; Secure Connection: close ~~~ HEARTBLEED: 2024/01/10 00:03:07 50.213.208.89:8443 - SAFE -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.213.208.89']

Name

98.160.48.170

Description

ISP: Cox Communications Inc. **OS:** None ----- Hostnames: -
wsip-98-160-48-170.dc.dc.cox.net ----- Domains: - cox.net
----- Services: **443:** ~~~ HTTP/1.1 200 OK Date: Sun, 07 Jan 2024 07:37:22
GMT X-Frame-Options: SAMEORIGIN Content-Type: text/html; charset=UTF-8 Expires: Wed, 31

Dec 1969 00:00:00 GMT Cache-Control: no-cache Pragma: no-cache Content-Length: 6445
 Set-Cookie: JSESSIONID=1uw5l7msc9mz14vfix5niq41m;Path=/corporate;HttpOnly;Secure Vary:
 Accept-Encoding ~~~ HEARTBLEED: 2024/01/06 23:39:50 98.160.48.170:443 - SAFE
 ----- **500:** ~~~ VPN (IKE) Initiator SPI: 666e626c7a347272 Responder SPI:
 6438303772643879 Next Payload: Notification (N) Version: 1.0 Exchange Type: Informational
 Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length:
 40 ~~~ -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '98.160.48.170']

Name

206.189.208.156

Description

ISP: DigitalOcean, LLC **OS:** Ubuntu ----- Hostnames:
 ----- Domains: ----- Services: **22:** ~~~ SSH-2.0-
 OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key:
 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEGILIGCgbbCG6yZ9QwTNK
 pA 0RKR95/lhsb7HupSzU8WcHHgBkcv3GT1cKGrCQWlsXW4xt785SU7GD0Xk8GbF3Q=
 Fingerprint: c1:dd:ec:e1:18:58:07:38:36:0b:1d:a7:9a:22:42:cd Kex Algorithms: curve25519-sha256
 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-
 hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256
 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519
 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr
 aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-
 etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com
 hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com
 umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression
 Algorithms: none zlib@openssh.com ~~~ -----

Pattern Type

stix

Pattern

[ipv4-addr:value = '206.189.208.156']

Malware

Name

CHAINLINE

Name

BUSHWALK

Name

GLASSTOKEN

Name

GIFTEDVISITOR

Name

LIGHTWIRE

Vulnerability

Name

CVE-2024-22024

Name

CVE-2024-21888

Name

CVE-2024-21893

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure), Ivanti Policy Secure, and Ivanti Neurons contain a server-side request forgery (SSRF) vulnerability in the SAML component that allows an attacker to access certain restricted resources without authentication.

Name

CVE-2024-21887

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure contain a command injection vulnerability in the web components of these products, which can allow an authenticated administrator to send crafted requests to

execute code on affected appliances. This vulnerability can be leveraged in conjunction with CVE-2023-46805, an authenticated bypass issue.

Name

CVE-2023-46805

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways contain an authentication bypass vulnerability in the web component that allows an attacker to access restricted resources by bypassing control checks. This vulnerability can be leveraged in conjunction with CVE-2024-21887, a command injection vulnerability.

Intrusion-Set

Name
UTA0178

Attack-Pattern

Name
TA0008
ID
TA0008
Name
TA0006
ID
TA0006
Name
TA0003
ID
TA0003
Name
T1078

ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and

the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the powershell.exe` binary through interfaces to PowerShell's underlying System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)`

Name

Exploitation for Client Execution

ID

T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ###

Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Name

T1505.003

ID

T1505.003

Description

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.(Citation: volexity_0day_sophos_FW) In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. [China Chopper](<https://attack.mitre.org/software/S0020>) Web shell client). (Citation: Lee 2013)

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion] (<https://attack.mitre.org/techniques/T1211>). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](<https://attack.mitre.org/techniques/T1611>), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

StixFile

Value

ed4b855941d6d7e07aacf016a2402c4c870876a050a4a547af194f5a9b47945f

e192932d834292478c9b1032543c53edfc2b252fdf7e27e4c438f4b249544eeb

9d901f1a494ffa98d967ee6ee30a46402c12a807ce425d5f51252eb69941d988

8bc8f4da98ee05c9d403d2cb76097818de0b524d90bea8ed846615e42cb031d2

26cbb54b1feb75fe008e36285334d747428f80aacdb57badf294e597f3e9430d

IPv4-Addr

Value

46.8.68.100

88.119.169.227

103.13.28.40

45.61.136.14

186.179.39.235

8.137.112.245

159.65.130.146

146.0.228.66

91.92.254.14

173.53.43.7

71.127.149.194

64.24.179.210

50.243.177.161

73.128.178.221

75.145.224.109

50.215.39.49

75.145.243.85

173.220.106.166

47.207.9.89

98.160.48.170

50.213.208.89

206.189.208.156

Domain-Name

Value

secure-cama.com

areekaweb.com

line-api.com

duorhytm.fun

clicko.click

clickcom.click

entraide-internationale.fr

miltonhouse.nl

dslogconfig.pm

webb-institute.com

gpoaccess.com

sessionserver.pl

Hostname

Value

cpanel.netbar.org

api.d-n-s.name

External References

-
- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b>
-
- <https://otx.alienvault.com/pulse/65e1a5b18d307f0d4139697b>