Feb 15 2024

NETMANAGEIT

Intelligence Report

Zero-day vulnerability in Ivanti software

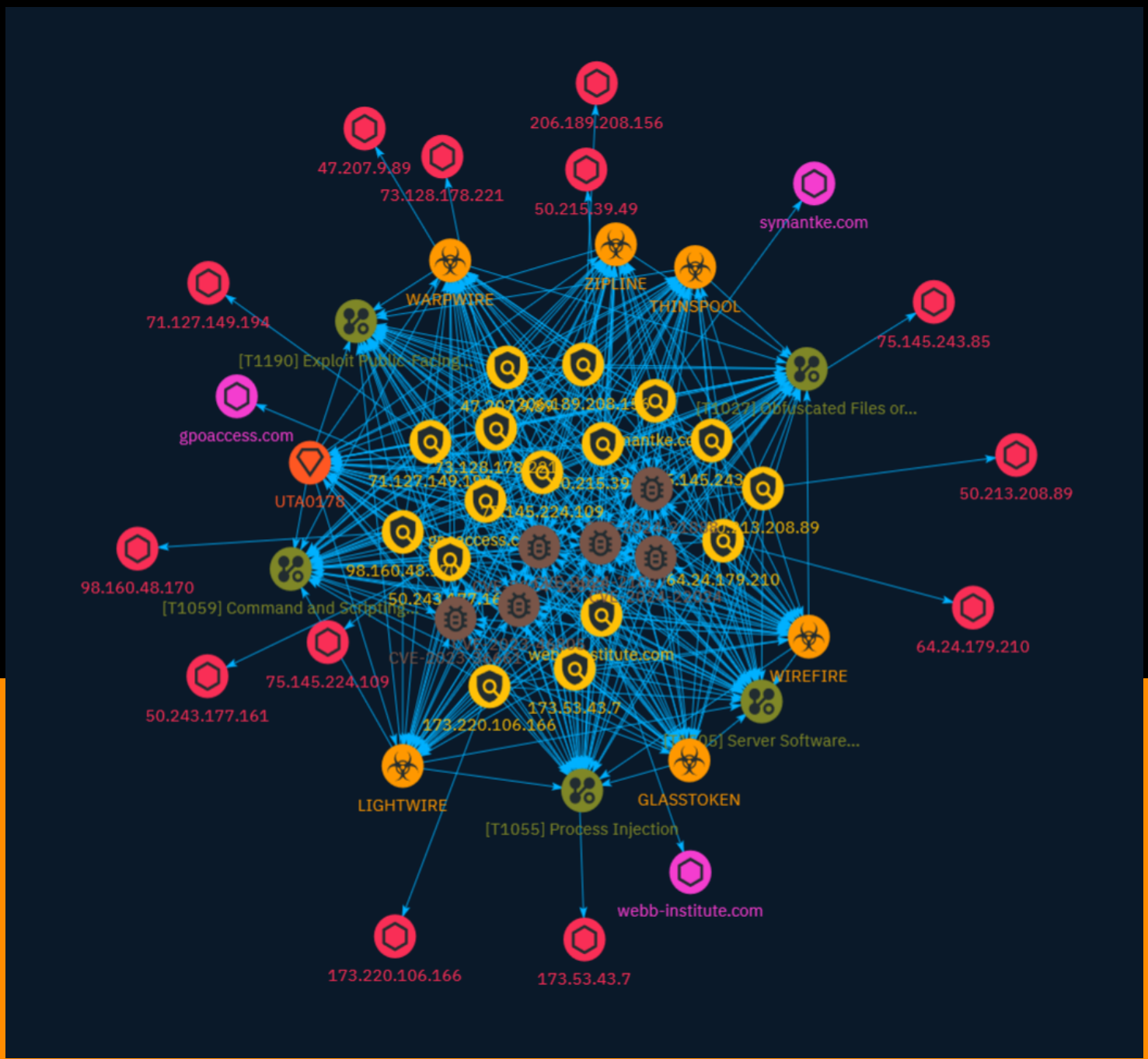

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Several actively exploited 0-day vulnerabilities were discovered in Ivanti products, including Ivanti Connect Secure and Ivanti Policy Secure. The vulnerabilities allow unauthenticated remote code execution and have been exploited by threat actors to install webshells and steal credentials. Ivanti has released patches and mitigations to address the issues. Organizations using vulnerable Ivanti products are advised to apply patches or mitigations as soon as possible and investigate for signs of compromise.

Confidence

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

15 / 100

Content

N/A

Vulnerability

Name
CVE-2024-22024
Name
CVE-2023-36661
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.

Malware

Name
ZIPLINE
Name
GLASSTOKEN
Name
WARPWIRE
Name
WIREFIRE
Name
LIGHTWIRE
Name
THINSPOOL

Intrusion-Set

Name
UTA0178

Indicator

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

symantke.com

Description

WARPWIRE C2 server

Pattern Type

stix

Pattern

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

Name

173.53.43.7

Description

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 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: AAAAB3NzaC1yc2EAAAADAQABAAABAQCKs+wiVy5mwX/5pDvaa5NpHDonmlIKyNY7ShPREkMBqVv1 OwMmlvJeFmW1Af7zSDNkdKqv4l/kZ8TofTStz6jAmYwmy1bTfbB8TRhNSEKDa72ULQUWKuIFlhZEwl2iMJ9EgAiDJj4shoXUMhmQ1GOoMsPQRtmjg4ybP4ylPEQsRZ04GpXD2JBYTHuCyV8wcvRSg/VTb076McAku1G3EKJecmqm9CIQNYCZvqYuOIewqt/2k3k/zz+IavWGmTYK/FeZgwCKBZYE2cWcT5Xb G9aGMUuO7X8cYYd8/h1vQhdYRRQxynBptd42xaMXbOEX3Kxoaa1/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=1tddjenmo7v6g14dlbzdmvgunk;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: AAAAB3NzaC1yc2EAAAADAQABAAAAgnXPHgULMdoHD+/ 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:

AAAAB3NzaC1yc2EAAAADAQABAAABAQCbei7INntyM2SqHAO1BIvV+KnxRA4yA7I2/uUeF6DJZNtD 8A0VLcN3pwJURNE03caxcfqmtYW+NEksKnKYbJTl5oMZxG8s2okz579YYI97n18rp9C+h+cB7vau VdTsBNDfpeW3sOYC4m/g0gbOEsGJnuJBCYEy2mL0o2fpj/d90FT3MqjaK3MhQsof2+Cq/5MD4r1J PFOta8AtgZkoG0hJi685AKv8ks4nnrd03JGEHWU6li4qWqlfbwBq/Vt7wo3xcf7ojyDxt2VJKk7n AI1jFG5uCJH/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: AAAAB3NzaC1yc2EAAAADAQABAAABAQCKs+wiVy5mwX/5pDvaa5NpHDonmlIKyNY7ShPREkMBqVv1 OwMmlvJeFmW1Af7zSDNkdKqv4l/kZ8TofTStz6jAmYwmy1bTfbB8TRhNSEKDa72ULQUWKuIFlhZE wl2iMJ9EgAiDJj4shoXUMhmQ1GOoMsPQRtmjg4ybP4ylPEQsRZ04GpXD2JBYTHuCyV8wcvRSg/VT b076McAku1G3EKJecmqm9CIQNYCZvqYuOIewqt/2k3k/zz+IavWGmTYK/FeZgwCKBZYE2cWcT5Xb G9aGMUuO7X8cYYd8/h1vQhdYRRQxynBptd42xaMXbOEX3Kxoaa1/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: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEGILIGCgbbCG6yZ9QwTNKpA 0RKr95/Ihsb7HupSzU8WcHHgBkcv3GT1cKGrCQWlsXW4xt785SU7GD0Xk8GbF3Q= 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']

Attack-Pattern

Name
Server Software Component
ID
T1505
Description
Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW)
Name
Command and Scripting Interpreter
ID
T1059
Description
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come

with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon

Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Exploit Public-Facing Application

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)

Domain-Name

Value
webb-institute.com
gpoaccess.com
symantke.com

IPv4-Addr

Value
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

External References

- https://www.orangecyberdefense.com/ch/blog/cybersecurity/ivanti-0-day
- https://otx.alienvault.com/pulse/65cc8b23585db393574cc9d4