Jan 16 2024

NETMANAGEIT

Intelligence Report

Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

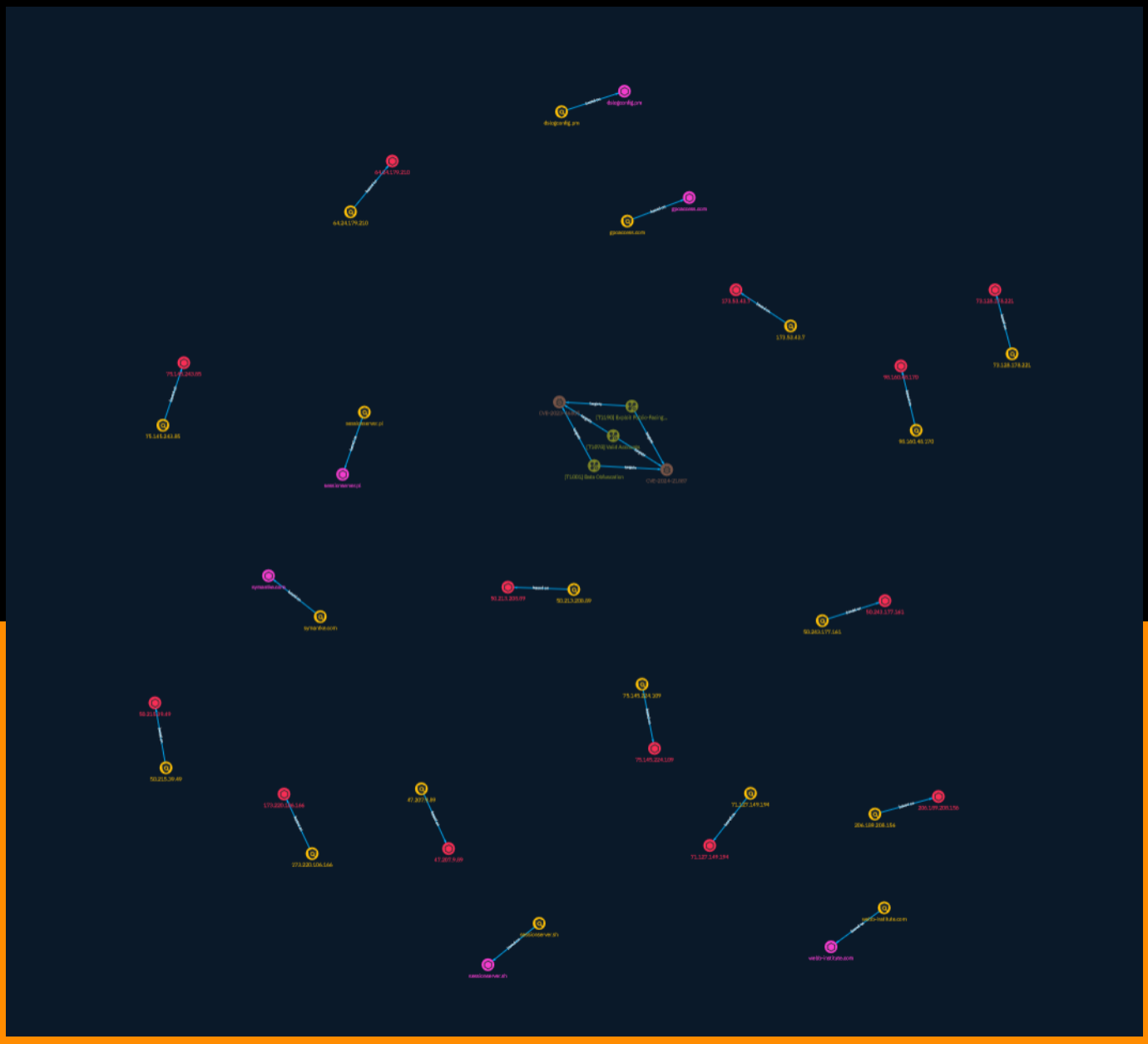

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Volexity has uncovered active in-the-wild exploitation of two vulnerabilities allowing unauthenticated remote code execution in Ivanti Connect Secure VPN appliances. An official security advisory and knowledge base article have been released by Ivanti that includes mitigation that should be applied immediately. However, a mitigation does not remedy a past or ongoing compromise. Systems should simultaneously be thoroughly analyzed per details in this post to look for signs of a breach.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Valid Accounts
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

Data Obfuscation

ID

T1001

Description

Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

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)

Indicator

Name

sessionserver.sh

Pattern Type

stix

Pattern

[domain-name:value = 'sessionserver.sh']

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

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

symantke.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1661062320, 'iso': '2022-08-21T02:12:00-04:00'} - **IPQS: Domain:** symantke.com - **IPQS: IP Address:** 172.67.210.161

Pattern Type

stix

Pattern

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

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

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

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

sessionserver.pl

Pattern Type

stix

Pattern

[domain-name:value = 'sessionserver.pl']

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']

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

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

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

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

webb-institute.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1683276754, 'iso': '2023-05-05T04:52:34-04:00'} - **IPQS: Domain:** webb-institute.com - **IPQS: IP Address:** 143.198.84.113

Pattern Type

stix

Pattern

[domain-name:value = 'webb-institute.com']

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
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

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/uUeF6DJZNtD8A0VLcN3pwJURNE03caxcfqmtYW+NEksKnKYbJTl5oMZxG8s2okz579YYI97n18rp9C+h+cB7vauVdTsBNDfpeW3sOYC4m/g0gbOEsGJnuJBCYEy2mL0o2fpj/d90FT3MqjaK3MhQsof2+Cq/5MD4r1JPFOta8AtgZkoG0hJi685AKv8ks4nnrd03JGEHWU6li4qWqlfbwBq/Vt7wo3xcf7ojyDxt2VJKk7nAI1jFG5uCJH/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

gpoaccess.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1683276862, 'iso': '2023-05-05T04:54:22-04:00'} - **IPQS: Domain:** gpoaccess.com - **IPQS: IP Address:** 143.198.84.113

Pattern Type

stix

Pattern

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

Vulnerability

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.

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.

Domain-Name

Value
sessionserver.pl
dslogconfig.pm
webb-institute.com
symantke.com
gpoaccess.com
sessionserver.sh

IPv4-Addr

Value
173.53.43.7
206.189.208.156
173.220.106.166
98.160.48.170
71.127.149.194
75.145.243.85
50.243.177.161
50.213.208.89
64.24.179.210
75.145.224.109
50.215.39.49
73.128.178.221
47.207.9.89

External References

- https://otx.alienvault.com/pulse/659fb93f559850df3e48609f
- https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/