Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

**SCHWACHSTELLE** | GEFÄHRDUNG | VORFALL | IT-ASSETS

# Zero-Day Schwachstellen bei Cyber-Angriffen auf verschiedene Ivanti-Produkte genutzt

*Nr. 2024-205101-1222, Version 1.2, 31.01.2024*

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

**TLP:CLEAR: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

## Sachverhalt

Am Abend des 10. Januar 2024 veröffentlichte der Hersteller Ivanti ein Advisory [IVAN24a] zu zwei bislang ungepatchten Schwachstellen in mehreren Produkten, die bereits für Cyber-Angriffe ausgenutzt werden.

Betroffen sind demnach folgende Lösungen:

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

Grundsätzlich sind **alle derzeit im Support befindlichen Versionen dieser Produkte betroffen**. Für ältere, nicht mehr unterstützte Patchstände hat der Hersteller bislang keine Untersuchungen vorgenommen. [IVAN24b]

In Ivantis Neurons for ZTA Gateways liegen die Schwachstellen zwar grundsätzlich vor, können im laufenden Betrieb bislang jedoch nicht angegriffen werden.

Bei den entdeckten Attacken kombinierten Angreifende eine Authentication Bypass- (CVE-2023-46805) (CVSS-Bewertung: 8.2) und eine Command Injection-Schwachstelle (CVE-2024-21887) (CVSS-Bewertung:

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

9.1) miteinander, um aus der Ferne Schadcode auf den Ivanti-Geräten auszuführen. Der Hersteller berichtet von Angriffen auf weniger als 10 Kunden [IVAN24b].

In einem Blogbeitrag von Volexity [VOLEX24] werden Details zum Ablauf der Angriffe veröffentlicht, die erstmals Anfang Dezember 2023 detektiert werden konnten.

**Update 1:**
Volexity veröffentlichte am 15. Januar 2024 einen Blogbeitrag über eine breite Ausnutzung der Schwachstellen. Mehr als 1.700 kompromittierte Ivanti Connect Secure Instanzen konnten von Volexity weltweit identifiziert werden. Die kompromittierten Systeme wurden in verschiedenen Sektoren wie Militär, Verteidigung, Regierung sowie in der Finanz- und Technologiebranche aufgefunden. Dabei geht Volexity davon aus, dass mehrere Gruppen hinter den Angriffen stecken. [VOLEX24b]

**Update 2:**
Am 31. Januar 2024 informierte der Hersteller über die Entdeckung einer neuen Privilege Escalation (CVE-2024-21888) sowie einer Server Side Request Forgery (SSRF) Schwachstelle (CVE-2024-21893) in den o.g. Produkten. Ivanti gibt an, dass die SSRF **Schwachstelle (CVE-2024-21893)**, die Angreifenden ohne Authentifizierung Zugriff auf bestimmte Ressourcen erlaubt, **bereits ausgenutzt wurde**.

Ivanti hat inzwischen erste Patches für Ivanti Connect Secure veröffentlicht, die schnellstmöglichst installiert werden sollten – siehe Abschnitt "Maßnahmen". Ebenso steht eine neue Mitigationsmaßnahme zur Verfügung, die, falls kein Patch installiert werden kann, eingespielt werden sollte. [IVAN24a]

Es werden weiterhin kompromittierte Ivanti Instanzen in Deutschland beobachtet [SHAD24]. Das BSI hat ebenso Kenntnis über mehrere kompromittierte Systeme.

# Bewertung

Das BSI geht aufgrund der branchenübergreifenden und weiten Verbreitung der genannten Produkte von einer hohen Betroffenheit durch die Sicherheitslücken aus [IVAN24d]. Bereits in der Vergangenheit (2021) warnte das BSI daher vor verwundbaren Connect Secure Gateways [BSI21], die für Angreifende attraktive Einfallstore in Netzwerke von zahlreichen Institutionen darstellen.

Die Angriffe mit Zero-Day Schwachstellen lassen darüber hinaus darauf schließen, dass Angreifende am Werk sind, die über umfangreiche Ressourcen verfügen.

Mit der kurzfristigen Veröffentlichung der Sicherheitslücken durch Ivanti ist davon auszugehen, dass weitere Akteure Angriffsversuche unternehmen werden.

**Update 1:**
Aufgrund der beobachteten breiten Ausnutzung der Schwachstelle seit dem 11. Januar [VOLEX24b] ist von einer bereits stattgefundenen Kompromittierung auszugehen, sollten zuvor keine Mitigationsmaßnahmen getroffen worden sein. **Eine Prüfung auf eine Kompromittierung ist daher notwendig.**

**Update 2:**
Dem BSI wurden kompromittierte Systeme in Deutschland gemeldet. Sofern die Meldungen an das Bundesamt nicht von den Betroffenen selbst, sondern über Partner erfolgten, wurden die zuständigen Stellen anschließend durch das BSI benachrichtigt. Ungeschützte Systeme werden von einer Vielzahl an Schadwaretypen [ORAN24], darunter mittlerweile auch Cryptominer, infiziert [GREY24].

Nach neuen Erkenntnissen sind die Angreifer in der Lage die vorherige Mitigationsmaßnahme und Erkennungsmaßnahmen (auch die externen Integritätsprüfung) zu umgehen. Ebenso wurden Ausbreitungen in interne Netzwerke und auf weitere Systeme durch die Angreifenden beobachtet. [CISA24]

Durch die neuen Schwachstellen, insbesondere durch CVE-2024-21893, sind **alle bisher mitigierten Systeme erneut gefährdet**.

Eine **breite Ausnutzung der neuen Schwachstelle CVE-2024-21893 ist zu erwarten.** [IVAN24b]

# Maßnahmen

IT-Sicherheitsverantwortliche sollten schnellstmöglich die Betroffenheit der eigenen Organisation prüfen und den von Ivanti bereitgestellten Workaround umsetzen, bis Patches verfügbar sind. Das Anwenden des Workarounds kann jedoch zu Einschränkungen in der Funktionalität [IVAN24b] führen.

## Workaround

Ivanti Kunden können die Mitigations XML-Datei (mitigation.release.20240107.1.xml) im Download Portal (nach Anmeldung) [IVAN24e] herunterladen.

Die XML-Datei kann dann wie folgt importiert werden (kein Neustart notwendig):

1. Navigieren Sie zu Maintenance > Import/Export > Import XML
2. Klicken Sie auf den Button "Browse" und wählen Sie die XML-Datei aus
3. Zum Abschluss klicken Sie auf den Button "Import"

Für Ivanti Connect Secure ergeben sich im Folgenden Einschränkungen für die Admin REST Automatisierungs-Funktionalität, die erweiterte HTML5-Funktionalität im Endnutzer-Portal, für die JSAM Funktionalität, die Rewriter Funktionalität, den Auto-Launch von PSAL Install und die Admin CRL Konfiguration. [IVAN24b]

Für Ivanti Policy Secure kommt es durch den Workaround zu einer signifikanten Verschlechterung des (Remote) Profiler, die Authentifikation zu IPS Instanzen wird jedoch weiterhin ermöglicht, außerdem ist UEBA adaptive Authentifikation nicht mehr verfügbar. [IVAN24b]

## Analyse

Aufgrund der beobachteten Angriffe sollten genutzte Ivanti-Lösungen auf eine bereits erfolgte Kompromittierung geprüft werden. Hierfür kann einerseits das Tool zur Integritätsprüfung genutzt werden, das bereits zum Funktionsumfang der Ivanti-Produkte gehört. Dieses überprüft jedoch lediglich die Integrität und kann Veränderungen am Dateisystem aufzeigen, es führt keinen Scan nach Schadware oder Indikatoren einer Kompromittierung durch.

Ivanti gibt an, dass Angreifende versucht haben, dieses Tool zu umgehen, dabei jedoch nicht erfolgreich war. IT-Sicherheitsverantwortliche sollten die Logs auf fehlgeschlagene Integritätsprüfung in der Vergangenheit überprüfen.

Der starker Indikator einer Kompromittierung liegt insbesondere dann vor, wenn die Logeinträge des internen Integritäts-Checks folgende Einträge aufweisen [VOLEX24]:

- SYS32039 - Es wurden mit dem Internal Integrity Check Tool neue Dateien gefunden
- SYS32040 - Es wurden mit dem Internal Integrity Check Tool veränderte Dateien gefunden

Es existiert ebenso ein externes Integritätsprüfungs-Tool [IVAN24c]. Dieses kann von Angreifenden nicht umgangen werden, jedoch erfordert die Analyse einen Neustart des Systems. Es wird empfohlen mit diesem Tool auf eine stattgefundene Kompromittierung zu prüfen.

Sollten Angreifende das System wieder von allen Veränderungen bereinigt haben, so kann keine Kompromittierung mit den Tools mehr festgestellt werden.

Auch sollte der Netzwerkverkehr auf Anomalien geprüft werden.

Das Threat-Intelligence Team von Volexity hat in einem Blogbeitrag [VOLEX24] weitere Details zu den Angriffen sowie Indikatoren zur Kompromittierung (IoCs) veröffentlicht und wird diesen ggf. um neue Indikatoren aktualisieren.
Der Blogbeitrag [VOLEX24] sollten von IT-Sicherheitsverantwortlichen ebenfalls genutzt werden, um auf eine stattgefundene Kompromittierung zu prüfen.

**Update 2:**
Es sollten **so schnell wie möglich die verfügbaren Patches** für Ivanti Connect Secure der Versionen

- 9.1R14.4
- 9.1R17.2
- 9.1R18.3
- 22.4R2.2
- 22.5R1.1

installiert werden, **um vor neuen Schwachstellen (CVE-2024-21888, CVE-2024-21893) geschützt zu sein.**

Nutzende der Software können die Patches im Download-Portal auffinden [IVAN24b]. Ebenso ist für Ivanti Neurons for ZTA Version 22.6R1.3 verfügbar. Für Ivanti Policy Secure werden Patches erst später veröffentlicht.

Sollte eine Version im Einsatz sein, zu der aktuell kein Patch zur Verfügung steht, so muss die Mitigation (mitigation.release.20240126.5.xml) [IVAN24b] angewandt werden, die mit erheblichen Funktionseinschränkungen einhergeht. Ein Upgrade auf eine aktuelle Version sollte durchgeführt oder das System vorübergehend abgeschaltet werden, bis ein sicherer Betrieb durch Patches wieder möglich ist. Wenn ein System gepatcht wurde, ist keine Mitigation mehr notwendig. Diese kann, falls vorhanden, entfernt werden [IVAN24b].

Für weitere, im Support befindliche Software-Versionen wird der Hersteller in den kommenden Tagen weitere Patches veröffentlichen. Nutzenden von Ivanti Connect Secure Versionen, deren Lösungenbereits ihr End of Life (EoL) erreicht haben, wird dringend empfohlen, ein Upgrade anzustoßen oder die Produkte auszusondern.

**Vor der Installation der Patches sollten alle Lösungen zurückgesetzt werden** (siehe [IVAN24b]) und anschließend alle hinterlegten Passwörter und Zertifikate ausgetauscht werden. Nur so kann eine Kompromittierung nachhaltig ausgeschlossen werden.

Sollte ein Zurücksetzen des Ivanti Systems unter keinen Umständen möglich sein, so sollte mindestens nach dem Installieren des Patches eine Integritätsprüfung mit dem externen Integritätsprüfungs-Tool [IVAN24c] durchgeführt werden, um eine vorherige Kompromittierung mit erhöhter Wahrscheinlichkeit auszuschließen (Updates für dieses Tool folgen zeitnah). Absolute Sicherheit bietet dieses Vorgehen jedoch nicht, da beobachtete Schadware zum Teil in der Lage war, den internen Integritätsprüfungsdienst zu deaktivieren [VOLEX24b][QUOI24] und den Externen zu umgehen [CISA24]. Ivanti veröffentlichte ebenfalls einen Guide zur Wiederherstellung nach einer Kompromittierung [IVAN24f].

Es wird dringend empfohlen, Systeme, die mit den Ivanti Lösungen in Verbindung stehen, genauer zu untersuchen und eine mögliche Ausbreitung des Angreifers auf interne Systeme zu prüfen. Dies betrifft insbesondere die Nutzung von Accounts bzw. das Verhalten bei Authentifizierungs-Vorgängen auf diesen Systemen.

Weiterhin kann die von Ivanti bereitgestellte Mitigationsanleitung [IVAN24b] genutzt werden, um das Risiko einer Ausnutzung der am 31. Januar veröffentlichten Schwachstellen zu reduzieren. Die Installation der Updates sollte jedoch mit Priorität verfolgt werden.

Falls eine Kompromittierung festgestellt wird, ist eine forensische Sicherung und anschließende Untersuchung durchzuführen.

Bei weiteren Fragen zur Vorfallbewältigung kann auch der Hersteller selbst direkt unter security@ivanti.com kontaktiert werden.

~~Der vorliegende Sachverhalt wird dadurch erschwert, dass zum aktuellen Zeitpunkt noch keine Updates zur Verfügung stehen, die die Schwachstellen schließen.~~ Ivanti hat angekündigt, diese für die einzelnen Produkte und Softwareversionen sukzessive zu veröffentlichen. Erste Patches werden für KW4 erwartet, bis Mitte Februar sollen dann alle betroffenen Produkte mithilfe von Updates abgesichert werden können.

IT-Sicherheitsverantwortliche sollten daher die Informationskanäle des Herstellers [IVAN24a][IVAN24b] regelmäßig auf neue Informationen zu verfügbaren Patches und IoCs prüfen. Weiterhin sollte die oben beschriebene Integritätsprüfung wiederkehrend durchgeführt werden, bis die o.g. Mitigationsmaßnahmen umgesetzt oder das Update in der eigenen Institution ausgerollt wurde.

# Links

[IVAN24a] Ivanti Security Advisory

https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

[IVAN24b] Ivanti Knowledge Base Article

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

[IVAN24c] Details on the External Integrity Check

https://forums.ivanti.com/s/article/KB44755

[IVAN24d] Ivanti Connect Secure VPN

https://www.ivanti.com/de/products/connect-secure-vpn

[IVAN24e] Ivanti Mitigation Download (Anmeldung notwendig)

https://forums.ivanti.com/s/article/Download-Links-Related-to-CVE-2023-46805-and-CVE-2024-21887

[BSI21] CSW - Remote-Code-Schwachstelle in PulseConnect Secure SSL-VPN-Gateway

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-208085-14M02.pdf

[VOLEX24] Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

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

**Update 1:**

[VOLEX24b] Ivanti Connect Secure VPN Exploitation Goes Global

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

**Update 2:**

[CISA24] New Mitigations to Defend Against Exploitation of Ivanti Connect Secure

https://www.cisa.gov/news-events/alerts/2024/01/30/new-mitigations-defend-against-exploitation-ivanti-connect-secure-and-policy-secure-gateways

[IVAN24f] Recovery Steps related to CVE-2023-46805 and CVE-2024-21887

https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887

[SHAD24] Shadow Server Reports

https://www.shadowserver.org/what-we-do/network-reporting/compromised-website-report/

[VOLEX24c] Ivanti Connect Secure VPN Exploitation: New Observations

https://www.volexity.com/blog/2024/01/18/ivanti-connect-secure-vpn-exploitation-new-observations/

[QUOI24] UNC5221: Unreported and Undetected WIREFIRE Web Shell Variant

https://quointelligence.eu/2024/01/unc5221-unreported-and-undetected-wirefire-web-shell-variant/

[GREY24] Ivanti Connect Secure Exploited to Install Cryptominers

https://www.greynoise.io/blog/ivanti-connect-secure-exploited-to-install-cryptominers

[ORAN24] Ivanti Connect Secure orange Cyberdefence Blogbeitrag

https://www.orangecyberdefense.com/global/blog/cybersecurity/ivanti

# Anlagen

## Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

## Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

    **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
    Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

## Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.