



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

# Remote-Code-Schwachstelle in Pulse Connect Secure SSL-VPN-Gateway

*Gezielte Angriffe in unterschiedlichen Branchen*

CSW-Nr. 2021-208085-14M02, Version 1.4, 25.05.2021

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:WHITE: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE 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

Es besteht eine Zero-Day-Schwachstelle im Pulse Connect Secure (PCS) SSL-VPN-Gateway des Herstellers Ivanti. Die Sicherheitslücke (CVE-2021-22893) erlaubt einem nicht authentifizierten Angreifer über die aus dem Internet erreichbare Webschnittstelle mittels Remote Code Execution (RCE) beliebigen Code auf dem PCS-Gateway auszuführen. Diese Sicherheitslücke hat den höchstmöglichen CVSS-Wert 10.0 [PSE2021a].

Derzeit gibt es noch kein Sicherheitsupdate für die oben genannte PCS 9.0R3 bis 9.1R11.3 betreffende Schwachstelle. Ivanti stellt einen Workaround zur Verfügung, der präparierte HTTP-Anfragen an die Webschnittstelle filtert. Mit Umsetzung des Workarounds sind einzelne Webdienste des PCS Gateways nicht mehr nutzbar.

Das IT-Sicherheitsunternehmen FireEye beobachtet die aktive Ausnutzung der Schwachstelle durch einzelne APT-Gruppen. Des Weiteren berichtet FireEye, dass ein Sicherheitsupdate für Anfang Mai 2021 geplant sei [FIR2021]. Die Cybersecurity & Infrastructure Security Agency (CISA) berichtet ebenfalls von einer aktiven Ausnutzung und dem Einsatz von WebShells für den Fernzugriff durch die Angreifenden [CIS2021a] und hat aufgrund des bestehenden Angriffsrisikos für Bundesbehörden eine Emergency Directive veröffentlicht [CIS2021b].

\* 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.

Das BSI hat Kenntnis über aktive Scans zur Suche nach PCS SSL-VPN-Gateways. Um nach möglichen Manipulationen auf Systemen zu suchen, stellt der Hersteller ein *PCS Integrity Tool* zur Verfügung [PSE2021b].

**Update 1:**

Kleinere sprachliche und inhaltliche Anpassungen im Text.

**Update 3:**

Laut Angaben des Herstellers Ivanti wird für die Sicherheitslücke CVE-2021-22893 am Montag den 03.05.21 um 15:00 CEST ein Update veröffentlicht. Zusätzlich wird bis voraussichtlich 17:00 CEST eine zugehörige Dokumentation veröffentlicht. Auf PCS Systemen, auf denen dies angewendet wurde, wird das Mitigationsskript mit der Installation des Patches v 9.1R11.4 automatisch wieder entfernt.

**Update 4:**

Im Mai veröffentlichte der Hersteller Ivanti Informationen bzgl. einer **neuen Buffer Overflow Schwachstelle (CVE-2021-22908)** inklusive zugehöriger Mitigationsmaßnahmen [PSE2021d]. **Als Patch für diese Schwachstelle wurde vom Hersteller für Ende Mai die Veröffentlichung der Version 9.1R11.5 angekündigt.**

## Bewertung

Das BSI geht aufgrund der branchenübergreifenden Verbreitung in verschiedenen Branchen von einer hohen Betroffenheit aus. Bereits in der Vergangenheit warnte und informierte das BSI Netzbetreiber über verwundbare Pulse Secure Gateways mit älteren Schwachstellen. Diese Schwachstellen wurden im Rahmen erfolgreicher Cyber-Angriffe als Einfallstor in Organisationen ausgenutzt.

Es ist zudem davon auszugehen, dass im Falle einer Veröffentlichung von Angriffcode eine großflächigere Ausnutzung erfolgt.

Analog zu vergleichbaren Schwachstellen ist aufgrund der beobachteten Angriffsaktivität auch nach Verfügbarkeit und Installation der Sicherheitsupdates eine Prüfung auf eine bereits erfolgte Kompromittierung unerlässlich.

**Update 2:**

Laut [NCC2021] sind deutschlandweit mehrere hundert PCS Systeme verwundbar für die vorliegenden Schwachstellen. Zudem befinden sich zahlreiche Systeme in einem nicht mehr unterstützten End of Life (EOL) Zustand der eine zukünftige Aktualisierung verhindert.

**Update 4:**

Dem BSI liegen mittlerweile weitere Hinweise über auf einer initialen Ausnutzung der älteren PCS Schwachstellen basierende gezielte Angriffe vor.

## Maßnahmen

Das BSI empfiehlt dringend zu überprüfen, ob das betroffene Produkte im Einsatz ist. Falls ja, muss der Workaround umgehend installiert werden, um eine Kompromittierung zu verhindern. Des Weiteren ist eine **Integritätsprüfung des VPN-Gateways mit dem vom Hersteller bereitgestellten Pulse Connect Secure Integrity Tool** zwingend erforderlich. Insbesondere bei Auffälligkeiten sollte eine weitere mögliche Kompromittierung der internen Netze untersucht werden. Sofern dazu keine internen Ressourcen vorliegen, ist ein externer IT-Forensikdienstleister hinzuzuziehen.

Falls eine Kompromittierung des VPN-Gateways festgestellt wird, ist eine forensische Sicherung und anschließende Untersuchung durchzuführen.

Der Hersteller empfiehlt im Anschluss folgendes Vorgehen zwecks Wiederherstellung des VPN-Gateways:

1. Deaktivierung des externen Netzwerk-Interfaces
2. System- und Benutzerkonfiguration sichern
3. Zurücksetzen auf die Werkseinstellungen über die serielle Konsole
4. Update der Appliance auf die neueste Version

5. Wiederherstellung der gespeicherten Konfigurationen
6. Aktivierung des externen Netzwerk-Interfaces

Im Falle von Angriffsaktivitäten sollten als Mindestanforderungen alle Benutzer und Dienstpasswörter zurückgesetzt werden. Weitere Hinweise sind in den FAQs des Integrity Tools zu finden [PSE2021c].

#### Update 3:

Das BSI empfiehlt die **zeitnahe Anwendung des veröffentlichten Patches v 9.1R11.4**.

**Sollte der Patch nicht umgehend installiert werden können, sind die vom Hersteller benannten Mitigationsmaßnahmen anzuwenden.**

**Zwecks Detektion von Angriffsversuchen die ggf. bereits vor der Anwendung entsprechender Mitigationsmaßnahmen unternommen wurden, rät das BSI zu einer regelmäßigen Integritätsprüfung.**

#### Update 4:

Bis zur Veröffentlichung des Patches v 9.1R11.5 sind die vom Hersteller benannten Mitigationsmaßnahmen anzuwenden [PSE2021d].

## Links

[CIS2021a] - Exploitation of Pulse Connect Secure Vulnerabilities

<https://us-cert.cisa.gov/ncas/alerts/aa21-110a>

[CIS2021b] - CISA Issues Emergency Directive Requiring Federal Agencies to Check Pulse Connect Secure Products

<https://www.cisa.gov/news/2021/04/20/cisa-issues-emergency-directive-requiring-federal-agencies-check-pulse-connect>

[FIR2021] - Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day

<https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html>

[NCC2021] - A Census of Deployed Pulse Connect Secure (PCS) Versions

<https://research.nccgroup.com/2021/04/23/a-census-of-deployed-pulse-connect-secure-pcs-versions/>

[PSE2021a] - Out-of-Cycle Advisory: Pulse Connect Secure RCE Vulnerability (CVE-2021-22893)

[https://kb.pulsesecure.net/articles/Pulse\\_Security\\_Advisories/SA44784/](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/)

[PSE2021b] - KB44755 - Pulse Connect Secure (PCS) Integrity Assurance

[https://kb.pulsesecure.net/articles/Pulse\\_Secure\\_Article/KB44755](https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755)

[PSE2021c] - KB44764 - Customer FAQ: PCS Security Integrity Tool Enhancements

[https://kb.pulsesecure.net/articles/Pulse\\_Secure\\_Article/KB44764](https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44764)

[PSE2021d] - SA44800 - 2021-05: Out-of-Cycle Advisory: Pulse Connect Secure Buffer Overflow Vulnerability

[https://kb.pulsesecure.net/articles/Pulse\\_Security\\_Advisories/SA44800/](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44800/)

# 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 TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.
- 2) Welche Einstufungen existieren?
  - **TLP:WHITE: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
  - **TLP:GREEN: Organisationsübergreifende Weitergabe**

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
  - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**

Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. 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. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
- 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:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.