



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

# Cisco VPN Geheimnisse in Klartext auslesbar

CSW-Nr. 2023-196940-1032, Version 1.0, 19.01.2023

IT-Bedrohungslage\*: 2 / Gelb

**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

Geräte, die mit den von Cisco vertriebenen Betriebssystemen Cisco IOS und Cisco IOS XE betrieben werden, können unter bestimmten Umständen Schlüsselmateriale im Klartext ausgeben. Bei Cisco IOS und Cisco IOS XE handelt es sich um die Standard-Betriebssysteme für Cisco-Netzwerkinfrastruktursysteme, welche weit verbreitet sind.

Aufgrund von Exportbeschränkungen werden die Betriebssysteme jeweils in zwei Versionen vertrieben: Eine hiervon unterstützt die Verschlüsselung von Netzwerk-Nutzdaten (universalk9), während der anderen (universalk9\_npe) die meisten kryptographischen Funktionen fehlen. Letztere wird daher als "No Payload Encryption" (NPE) Version bezeichnet. Das Aufspielen des jeweiligen Installationsimages bestimmt somit die Verfügbarkeit der Kryptographiemodule.

Eine Ausführung von Befehlen zur Konfiguration von kryptographischen Funktionen auf einem NPE-System führt zu einer Fehlermeldung auf der jeweiligen Kommandozeile. Im Falle des Einlesens der zuletzt gespeicherten Konfiguration (startup-config) während des Bootvorgangs geschieht dies auf der Konsole. In dieser Fehlermeldung können vertrauliche Informationen, wie beispielsweise Schlüsselmateriale für VPN-Verbindungen, im Klartext ausgegeben werden. Voraussetzung hierfür ist, dass ein System mit bestehender Konfiguration für eine betroffene kryptographische Funktion mit einem NPE-Image gestartet wird. Dies ist unter anderem möglich, wenn:

- neben dem universalk9 auch ein universalk9\_npe Image auf dem Gerät vorhanden ist,

\* 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.

- ein universalk9\_npe während des Startvorgangs per TFTP geladen wird oder
- ein universalk9\_npe während des Startvorgangs per USB geladen wird.

Folgende Funktionen zählt Cisco zur starken Nutzdatenverschlüsselung, welche in der NPE Version nicht vorhanden sind und deren Geheimnisse daher potentiell im Klartext ausgegeben werden können:

- Internet Protocol Security (IPsec) VPN
- LoRaWAN
- Media Access Control Security (MACsec)
- SD-WAN
- Secure StackWise Virtual
- Secure Unified Communications
- SSL VPN
- Wireless Personal Area Network (WPAN)

Weitere Informationen können dem Advisory von Cisco [CISCO2023] entnommen werden.

## Bewertung

Das BSI geht von einer weiten Verbreitung mit einer hohen Relevanz für alle Branchen aus. Derzeit liegen dem BSI keine Hinweise darauf vor, dass Angreifende bereits aktiv auf diese Weise Schlüsselmaterial erlangen.

Im Moment ist jedoch nicht von flächendeckenden Angriffen auszugehen, da der Zugriff auf die Kommandozeile oder physischer Zugang zu betroffenen Geräten benötigt wird. Einige der betroffenen Geräte sind speziell für den Remoteeinsatz konstruiert. Hierbei ist zu beachten, dass Angreifende sich unter Umständen leichter physischen Zugang verschaffen können. Darüber hinaus ist dem BSI bekannt, dass auch auf einigen Geräten, die in Deutschland verkauft wurden, universalk9\_npe Images zu finden waren.

Das erfolgreiche Auslesen von sensiblen und geheimen Daten, aus beispielsweise VPN Systemen, ist als nicht kompliziert und das Schadenspotential als hoch zu bewerten.

## Maßnahmen

Das BSI empfiehlt jedem Betreiber zu überprüfen, ob die betroffenen Produkte im Einsatz sind und die von Cisco beschriebenen Maßnahmen [CISCO2023] zeitnah zu berücksichtigen. Diese enthalten unter anderem Zugriffslimitierungen auf die Uploadfunktion für Softwareimages, als auch die sichere Speicherung von sensiblen und geheimen Daten durch weitere kryptographische Prozesse. Insbesondere sollte überprüft werden, ob auf den entsprechenden Geräten ein NPE-Image vorhanden ist und dieses entfernt werden, wenn es nicht benötigt wird.

Des Weiteren kann die Angriffsfläche durch eine konsequente Anwendung der Defense-in-Depth-Strategie und Härungsmaßnahmen minimiert werden [CISCO2020]. Hinweise hierzu finden sich auch im ICS-Kompendium des BSI [BSI2013].

## Links

[CISCO2023] - Cisco Security Advisory

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npe-hardening-Dkel83jP>

[BSI2013] - ICS Security Kompendium

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security\\_kompendium\\_pdf.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html)

[CISCO2020] - Cisco Guide to Harden Cisco IOS Devices

<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

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