Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstellen in Cisco Switches

CSW-Nr. 2023-231640-1032, Version 1.0, 22.05.2023

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

Am 17. Mai 2023 veröffentlichte der weltweite Marktführer im Bereich Netzwerkprodukte Cisco ein Advisory zu Schwachstellen in verschiedenen Produktfamilien von Switches [CISCO2023].

Die gefundenen Schwachstellen betreffen die web-basierte Benutzeroberfläche zur Verwaltung mehrerer Switches und wurden nach dem Common Vulnerability Scoring System (CVSS) v.3.1 als "kritisch" eingestuft.

Es handelt sich um folgende Schwachstellen:

- CVE-2023-20159, CVE-2023-20160, CVE-2023-20161 und CVE-2023-20189: Erlauben einem nicht-authentifizierten entfernten Angreifer die Ausführung von beliebigem Programmcode mit root-Rechten durch unzureichende Prüfung von Anfragen, die zu Speicherüberläufen (CWE-120) in Cisco Small Business Series Switches führen. Der Angreifer muss zur Ausnutzung der Schwachstellen eine präparierte Anfrage an die web-basierte Benutzeroberfläche schicken. Die genannten Sicherheitslücken werden von Cisco mit einem CVSS v.3.1 Score von 9.8 bewertet.
- Es existieren weitere Schwachstellen, die mit diesem Patch geschlossen werden, die unter anderem Denial-of-Service Angriffe ermöglichen.

Von den Schwachstellen sind folgende Produktreihen betroffen:

- 250 Series Smart Switches
- 350 Series Managed Switches

* 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.

- 350X Series Stackable Managed Switches
- 550X Series Stackable Managed Switches
- Business 250 Series Smart Switches
- Business 350 Series Managed Switches
- Small Business 200 Series Smart Switches
- Small Business 300 Series Managed Switches
- Small Business 500 Series Stackable Managed Switches

Die Reihen 220 Series Smart Switches und Business 220 Series Smart Switches sind nicht von den Schwachstellen betroffen.

Aufgrund des abgelaufenen Supports wird es für folgende Produktreihen keine Updates geben:

- Small Business 200 Series Smart Switches
- Small Business 300 Series Managed Switches
- Small Business 500 Series Stackable Managed Switches

Bewertung

Die große Verbreitung von Netzwerkprodukten der Firma Cisco stellt nach Einschätzung des BSI in Verbindung mit diversen "kritisch" eingestuften Sicherheitslücken ein erhöhtes Bedrohungspotential für Organisationen in Deutschland dar.

Die Schwachstellen CVE-2023-20159, CVE-2023-20160, CVE-2023-20161 und CVE-2023-20189 wurden von Cisco als kritisch eingestuft und sollten schnellstmöglich behandelt werden.

Eine kurzfristige Ausnutzung der Schwachstellen kann nicht ausgeschlossen werden, da Cisco davon berichtet, dass Proof-of-Concept Exploit-Code verfügbar ist.

Durch die zentrale Bedeutung der betroffenen Komponenten für IT-Netzwerke können Verfügbarkeit, Vertraulichkeit und Integrität in Institutionen kompromittiert werden.

Maßnahmen

Zunächst sollten die von Cisco Systems veröffentlichten Informationen ausführlich gesichtet und die genannten Komponenten mit der eigenen Inventarliste abgeglichen werden, um das Ausmaß der eigenen Betroffenheit zu identifizieren.

Weiterhin sollten die vom Hersteller bereitgestellten Patches zeitnah installiert werden, um einer möglichen Ausnutzung entgegen zu wirken. Es stehen keine Workarounds für die veröffentlichten Schwachstellen zur Verfügung, weshalb ein Schließen der Lücken nur durch das Einspielen der Patches möglich ist.

Vom Einsatz der nicht mehr unterstützten Produkte wird wegen der fehlenden Versorgung mit Sicherheitspatches abgeraten.

Grundsätzliche Empfehlungen zum sicheren Umgang mit Switches hat das BSI im IT-Grundschutz NET.3.1 zusammengefasst [BSIGS2021].

Links

[CISCO2023] Cisco Security Advisories https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv

[BSIGS2021] BSI Grundschutz NET.3.1 Router und Switches https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_1_Router_und_Switches_Edition_2021.pdf?__blob=publicationFile&v=2

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.