Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in Cisco Enterprise NFV Infrastructure Software

Nr. 2021-251660-1022, Version 1.0, 03.09.2021

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: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

Am 01.09.2021 veröffentlichte der Hersteller Cisco Informationen zu einer Schwachstelle in der Cisco Enterprise NFV Infrastructure Software (NFVIS) welche es entfernten, nicht authentifizierten Angreifern ermöglicht, administrativen Zugriff auf einem betroffenen Gerät zu erhalten (siehe [CIS2021]).

Mithilfe einer Sicherheitslücke in der TACACS Authentifizierungs-, Autorisierungs- und Abrechnungsfunktion (AAA) der NFVIS könnte ein Angreifer demnach aus der Ferne die Authentifizierung umgehen und sich als Administrator bei einem betroffenen Gerät anmelden (siehe [CIS2021]).

Diese Sicherheitsanfälligkeit ist auf eine unvollständige Validierung von Benutzereingaben zurückzuführen, die an ein Authentifizierungsskript übergeben werden. Angreifende können diesen Sachverhalt ausnutzen, indem Parameter in eine Authentifizierungsanforderung eingefügt werden (siehe [CIS2021]). Mit einem CVSS-Score von 9.8 gilt diese Schwachstelle (CVE-2021-34746) als "kritisch".

Betroffen sind nach Angaben des Herstellers Cisco Enterprise NFVIS mit der Version 4.5.1, **wenn TACACS als externe Authentifizierungsmethode aktiviert** wurde.

* 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.

Bewertung

Aufgrund des hohen Marktanteils von Cisco im Netzwerk-Bereich im Allgemeinen muss davon ausgegangen werden, dass auch das hier betroffene Produkt in zahlreichen Organisationen in Deutschland zum Einsatz kommt.

Dem BSI liegen aktuell noch keine Informationen einer aktiven Ausnutzung der Schwachstelle vor. Aufgrund des vor Kurzem veröffentlichten PoC und der Kritikalität sowie der Gegebenheit der Schwachstelle, ist die kurzfristige Erstellung von schadhaften Anwendungen basierend auf dem öffentlichen PoC nicht auszuschließen.

Maßnahmen

Cisco hat Software-Updates veröffentlicht, die diese Sicherheitsanfälligkeit beheben. Zielführende Mitigationsmaßnahmen sind zum aktuellen Zeitpunkt nicht bekannt, weshalb das Einspielen des bereitgestellten Patches priorisiert werden sollte.

Empfehlungen zum Ausrollen von Sicherheitsupdates im Allgemeinen können dem BSI IT-Grundschutz entnommen werden [BSI2021].

Links

[CIS2021] - Cisco Enterprise NFV Infrastructure Software Authentication Bypass Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-g2DMVVh

[BSI2021] - IT-Grundschutz OPS.1.1.3:Patch- und Änderungsmanagement
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2020.pdf

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.