Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Schwachstelle im Modul "mod_proxy" von Apache HTTP-Server

Nr. 2021-270312-1022, Version 1.0, 26.11.2021

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

Das Modul "mod_proxy" des Apache-Servers fungiert als Gateway-Komponente und unterstützt eine Vielzahl an Protokollen und Mechanismen zum Lastenausgleich (Load-Balancing) von Webdiensten wie Videokonferenzen. Dabei kann es als "Forward-Proxy" und als "Reverse-Proxy" zum Einsatz kommen.

Mit CVE-2021-40438 wurde eine "Server-Side Request Forgery" Schwachstelle bekannt, welche es entfernten und nicht authentifizierten Angreifenden mittels speziell präparierten uri-Path-Anfragen ermöglicht, den httpd-Server dazu zu bringen, diese Anfragen an beliebige Server weiterzuleiten.

Betroffen ist demnach auch die Videokonferenzlösung Cisco Expressway Series [CI2021].
Dem BSI ist mindestens ein Fall bekannt, bei dem es einem Angreifenden möglich war, durch Ausnutzung der Schwachstelle Hashwerte von Benutzer-Credentials vom System des Opfers zu erlangen.

Die Schwachstelle betrifft alle Versionen von Apache HTTP-Server 2.4.48 oder älter.

Bewertung

Angreifende können durch Ausnutzung der Schwachstelle Ressourcen unterschiedlicher Dienste, welche auf dem jeweiligen Webserver angeboten werden, an Dritte weiterleiten. In Abhängigkeit der Konfiguration des

* 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.

Apache-Httpd-Dienstes ist es möglich, auch solche Dienste zu ändern oder zu deaktivieren, welche durch eine Firewall separiert sein sollten.

Die Kritikalität der Schwachstelle wird mit einem Common Vulnerability Scoring System (CVSS)-Wert von 9.0 bewertet. Dies ist unter anderem mit der einfachen Ausnutzbarkeit und der Verfügbarkeit eines öffentlichen Proof of Concept (PoC) zu begründen (Anleitungen zur Ausnutzung der Schwachstelle [PO2021]).

Maßnahmen

Das BSI empfiehlt jedem Betreiber zu überprüfen, ob Produkte im Einsatz sind, die durch die Schwachstellen betroffen sind und die beschriebenen Maßnahmen der Hersteller bezüglich Updates und dem sicheren Betrieb der Systeme zeitnah zu berücksichtigen.

Informationen zu den durch Hersteller zur Verfügung gestellten Updates befinden sich auf dieser Seite [MI2021]. Eine alternative Mitigation erscheint nach derzeitigem Kenntnisstand nicht möglich.

Grundsätzliche Empfehlungen zum sicheren Betrieb von Webservern hat das BSI im IT-Grundschutz APP.3.2 zusammengefasst (siehe [BSI2021a]).

Das Kompendium Videokonferenzsysteme (KoViKo) richtet sich an Entscheider, Planer, Beschaffer, Betreiber, Administratoren, Auditoren und auch Endnutzer, die über Videokonferenz Inhalte beziehungsweise Informationen mit normalem und erhöhtem Schutzbedarf austauschen (siehe [BSI2021b]).

Links

[BSI2021a] - APP.3.2: Webserver
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/06_APP_Anwendungen/APP_3_2_Webserver_Edition_2021.pdf

[BSI2021b] - Kompendium Videokonferenzsysteme
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf

[CI2021] - Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products: November 2021
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-2.4.49-VWL69sWQ

[MI2021] - MITRE Eintrag CVE-2021-40438
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40438

[PO2021] - Building a POC for CVE-2021-40438
https://firzen.de/building-a-poc-for-cve-2021-40438

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.