Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in Apache Webserver "httpd"

Nr. 2021-260764-1122, Version 1.1, 08.10.2021

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

Der Apache Webserver "httpd" ist eine weit verbreitete Software zum Ausliefern von Webseiten. Das zugehörige Modul "mod_cgi" wird zur Bereitstellung von dynamischen Inhalten auf Basis von Skriptsprachen genutzt. In der Vergangenheit war dies der de-facto-Standard zur Anbindung von zum Beispiel Perl- und Python-basierten Webanwendungen.

Am 4.10.2021 veröffentliche Apache ein als "wichtig" gekennzeichnetes Sicherheitsupdate für den Apache "httpd", das CVE-2021-41773 schließt (siehe [APA2021a], [NVD2021]). Die Auswirkung der Schwachstelle wurde als "Path Traversal & Information Disclosure" beschrieben (siehe [APA2021a]). Verschiedene Medien berichteten inklusive eines Proof-of-Concept (PoC) über den Sachverhalt.

Am 6.10.2021 veröffentlichte das Sicherheitsunternehmen Rapid7 einen Blog-Eintrag, der darlegt, dass die Schwachstelle ebenfalls zur Ausführung von Betriebssystemkommandos durch unauthentifizierte Angreifende verwendet werden kann (siehe [RAP2021]).

Die Standardkonfiguration des "httpd" ist in Kombination mit dem aktivierten Modul "mod_cgi" für den Angriff verwundbar. Das Modul "mod_cgi" wird standardmäßig mit dem "httpd" ausgeliefert und hat in der Vergangenheit lange Zeit als Standard-Schnittstelle zwischen "httpd" und Skriptsprachen wie Perl oder Python gedient. Es ist wahrscheinlich, dass das Modul bei einem Teil der verwundbaren Instanzen aktiviert 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.

Einige Distributionen, beispielsweise Debian, liefern jedoch modifizierte Standardkonfigurationen aus, die auch in der Vergangenheit und mit aktiviertem "mod_cgi" nicht für die Schwachstelle verwundbar waren.

Update 1:
Apache informierte am 07.10.2021 darüber, dass das Update 2.4.50, das die CVE-2021-41773 beheben sollte, unzureichend war. Entsprechend vergab Apache die CVE-2021-42013 und veröffentlichte das Sicherheitsupdate 2.4.51, das nun die Schwachstelle beheben soll (siehe [MIT2021a], [APA2021a]).

Bewertung

Nach ersten Betrachtungen werden in Deutschland etwa 12.000 Systeme mit der verwundbaren Version 2.4.49 betrieben. Wie viele Systeme davon zusätzlich das Modul "mod_cgi" aktiviert haben, ist zur Zeit unklar. **Über eine aktive Ausnutzung der Lücke wird jedoch bereits berichtet.** Die veröffentlichten Proof-of-Concepts können leicht für Angriffe missbraucht werden und so zum Beispiel für Datenabfluss aus den betriebenen Webanwendungen und die **vollständige Übernahme des Servers** verwendet werden.

Sollte eine verwundbare Konfiguration vorliegen, ist davon auszugehen, dass diese Systeme bereits durch Angreifer kompromittiert worden sind.

Update 1:
Betroffen durch die CVE-2021-42013 sind ausschließlich Apache Webserver "httpd" in den Versionen 2.4.49 und 2.4.50, jedoch keine vorherigen Versionen (siehe [MIT2021a], [APA2021a]) .

Maßnahmen

Das BSI empfiehlt dringend, die aktuelle Version des Apache "httpd" einzuspielen, die vom Hersteller veröffentlicht worden ist. Diese kann über die für die entsprechende Distribution üblichen Update-Prozesse bezogen werden.

Die Konfiguration des Webservers sollte unabhängig vom Update eine Direktive enthalten (vgl. [APA2021b]), die den Zugriff auf das Wurzelverzeichnis grundsätzlich untersagt. Sollte diese Direktive - wie beispielsweise bei der mit Debian ausgelieferten Konfiguration - bereits vorhanden sein, ist die eingesetzte Konfiguration nicht für diese Schwachstelle verwundbar.

Von Apache wird die folgende Konfiguration empfohlen:

<Directory />

Require all denied

</Directory>

Sofern "mod_cgi" aktiviert ist, sollte überprüft werden, ob dies benötigt wird oder deaktiviert werden kann.

Sollte eine anfällige Konfiguration vorliegen und der Webserver aus dem Internet erreichbar sein, **ist davon auszugehen, dass die Systeme bereits kompromittiert wurden.** In diesem Fall sollten Backups eingespielt und Logs und verbundene Systeme auf Unregelmäßigkeiten geprüft werden. Die gegebenenfalls im Sicherheitskonzept vorgesehenen Maßnahmen im Falle einer Kompromittierung sollten unabhängig davon ergriffen werden.

Mögliche Maßnahmen im Falle einer Kompromittierung können sein:

- Potenziell infizierte Systeme sollten umgehend vom Netzwerk isoliert werden, um eine weitere Ausbreitung der Angreifenden im Netz durch Seitwärtsbewegungen (Lateral Movement) zu verhindern. Dazu das Netzwerkkabel ziehen. Gerät nicht herunterfahren oder ausschalten. Gegebenenfalls forensische Sicherung inkl. Speicherabbild für spätere Analysen (eigene, durch Dienstleister oder Strafverfolgungsbehörden) erstellen.
- Alle auf betroffenen Systemen gespeicherten bzw. nach der Infektion eingegebenen Zugangsdaten sollten als kompromittiert betrachtet und die Passwörter geändert werden. Dies umfasst u. a. Datenbanken, Applikationsserver, SSH und Fileserver etc.
- Prüfen Sie, ob Sie saubere, integre Backups haben.

Weitere Informationen wie Sie im Falle eines IT-Sicherheitsvorfalls reagieren sollten, finden Sie auf der Webseite des BSI in der Rubrik "IT-Sicherheitsvorfall" (siehe bspw. für Unternehmen [BSI2021a]).

Des Weiteren sollte der Webserver immer mit möglichst geringen Nutzerrechten ausgeführt werden und möglichst restriktive Security-Enhanced (SE)-Linux Beschränkungen konfiguriert haben.

Grundsätzliche Empfehlungen zum sicheren Betrieb von Webservern hat das BSI im IT-Grundschutz APP.3.2 zusammengefasst (siehe [BSI2021b]).

Links

[APA2021a] - Apache Security Tips
https://httpd.apache.org/security/vulnerabilities_24.html

[APA2021b] - Apache HTTP Server 2.4 vulnerabilities
http://httpd.apache.org/docs/current/misc/security_tips.html#protectserverfiles

[BSI2021a] - Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen_node.html

[BSI2021b] - 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

[NVD2021] - National Vulnerability Database CVE-2021-41773 Detail
https://nvd.nist.gov/vuln/detail/CVE-2021-41773

[RAP2021] - Apache HTTP Server CVE-2021-41773 Exploited in the Wild
https://www.rapid7.com/blog/post/2021/10/06/apache-http-server-cve-2021-41773-exploited-in-the-wild/

Update 1:
[MIT2021a] - CVE-2021-42013 Details
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42013

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.