Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in OpenSSL 3.0

Nr. 2022-267005-1122, Version 1.1, 01.11.2022

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

Die Kryptobibliothek OpenSSL wird seit mehreren Jahren in verschiedenen kryptographischen Systemen eingesetzt. Sie ist besonders wichtig bei gesicherten Datenübertragungen in Computernetzwerken und spielt aufgrund ihrer großen Verbreitung im Internet eine besonders wichtige Rolle bei der Verwendung von z.B. HTTPS (HTTP over SSL/TLS), aber auch bei VPN-Gateways. OpenSSL bietet eine große Zahl von kryptographischen Funktionen an; dazu gehören z.B. symmetrische und asymmetrische Datenverschlüsselung, digitale Signaturen, Authentisierung, Hashfunktionen, Erstellung und Verifikation von Zertifikaten inklusive Zertifikatsketten, Mechanismen zum Integritätsschutz, Schlüssel- und Zufallszahlenerzeugung. Die wichtigste Aufgabe von OpenSSL ist es jedoch, eine Implementierung des TLS-Protokolls (früher SSL-Protokoll) bereitzustellen.

Am 01.11.2022 plant das OpenSSL-Team einen Patch zu veröffentlichen, mit dem unter anderem eine kritische Schwachstelle in OpenSSL 3.0 behoben werden soll. Die Schwachstelle wird nach Angaben des Teams als kritisch eingeschätzt, weitere Details sind aktuell nicht bekannt. OpenSSL 3.0 findet in verschiedenen IT-Systemen und Linux Distributionen Verwendung.

Eine möglichst umfassende Liste von betroffenen und nicht betroffenen Produkten wird durch die internationale Community zusammengetragen und zentral durch das NCSC-NL auf GitHub gepflegt (siehe [GITH2022a]). Diese Liste wird bis auf Weiteres fortlaufend ergänzt werden.

* 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.

Update 1:
Das OpenSSL-Projekt hat OpenSSL 3.0.7[OPEN2022d] veröffentlicht. Diese Version schließt zwei schwerwiegende Schwachstellen, die Pufferüberläufe ermöglichen. Diese beiden Schwachstellen waren vor Veröffentlichung als eine Schwachstelle kritisch eingestuft worden; mit Blick auf verfügare Mitigationsstrategien wurde die Kritikalitätseinschätzung seitens des OpenSSL-Projekts leicht nach unten korrigiert [OPEN2022e].

Die durch den Patch behobenen schwerwiegenden Schwachstellen CVE-2022-3786 und CVE-2022-3602 betreffen den Punycode-Parser und erlauben jeweils einen Pufferüberlauf, der zu Nichtverfügbarkeit von Diensten und unter bestimmten Bedingungen zur Codeausführung genutzt werden kann. Die Schwachstellen betreffen das Parsen von E-Mail-Adressen in X.509-Zertifikaten nach der Zertifikatsvalidierung. Um die Schwachstellen ausnutzbar zu machen, muss ein Client auf einen maliziösen Server zugreifen oder ein maliziöser Client auf einen Server zugreifen, der ein Client-Zertifikat anfordert. Schlägt eine Validierung des maliziösen Zertifikats fehl, kann die Schwachstelle nicht ausgenutzt werden.

Bewertung

Die veröffentlichte Schwachstelle betrifft per Definition des OpenSSL Projektes (Kritikalität "kritisch") gängige Konfigurationen (vgl. [OPEN2022b]), jedoch sind nach aktuellem Kenntnisstand keine OpenSSL Versionen unter 3.0 betroffen. Aufgrund der Verbreitung und Einsatzmöglichkeit von OpenSSL ist eine größere Betroffenheit von IT-Systemen nicht auszuschließen.

Die Kryptobibliothek OpenSSL kann auch in IT-Anwendungen enthalten sein, die nicht die durch das Betriebssystem bereitgestellte Bibliothek verwenden. In diesen Fällen sind Patches durch die entsprechenden Hersteller notwendig.

Update 1:
Die Codeausführung sollte auf modernen Betriebssystemen bereits durch Sicherheitsechniken wie u.A. ASLR und NX mitigiert werden. Ein Denial-of-Service ist dennoch möglich. Ein Denial-of-Service betrifft in relevantem Ausmaß ausschließlich Server, zusätzlich müssen spezielle Bedingungen gegeben sein.

Die Bedingungen für einen erfolgreichen Angriff auf einen Serverdienst durch die Schwachstellen sind:

- Ein Client-Zertifikat wird angefordert,
- das Zertifikat ist valide oder die Zertifikatsvalidierung wird ignoriert,
- das Zertifikat enthält eine E-Mail-Adresse,
- OpenSSL 3.0.0 - 3.0.6 wird eingesetzt.

Maßnahmen

Der angekündigte Patch sollte gemäß Grundschutzbaustein OPS.1.1.3 (vgl. [BSI2021]) zeitnah eingespielt werden (siehe [GITH2022b]). Es ist daher empfohlen, sicherzustellen, dass am Patchtag autorisiertes IT-Personal zur Verfügung steht, welches das Update kurzfristig einspielen kann. Die Bereitstellung durch das Projekt wird zwischen 14 und 18 Uhr deutscher Zeit erwartet (siehe [OPEN2022c]).

Zusätzlich sollte erwogen werden, ob verwundbare Systeme vom Internet getrennt werden können und sollten, bis ein Patch zur Verfügung steht.

Zur Identifikation betroffener Produkte kann die Liste von NCSC-NL (vgl. [GITH2022a]) herangezogen werden.

Update 1:
Updates sollten, sobald sie für die entsprechenden Produkte und Betriebssysteme verfügbar sind, eingespielt werden. Serverdienste, die mTLS verwenden bzw. ein Client-Zertifikat anfordern, sollten auf Verfügbarkeitsprobleme überwacht werden. Betroffene Systeme, die keine aktiven Mitigationen für Stack Overflow Angriffe bieten, sollten zusätzlich auf Anzeichen von Schadcodeausführung überwacht oder bis zur Installation des Patches vom Internet getrennt werden.

Auf [GITH2022a] finden sich neben der Liste von betroffenen Produkten auch eine Reihe von Skripten und Tools, die genutzt werden können, um betroffene OpenSSL Bibliotheken zu finden.

Links

[BSI2021] - Grundschutzbaustein OPS.1.1.3
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021.html

[GITH2022a] - GitHub Liste der betroffenen Produkte
https://github.com/NCSC-NL/OpenSSL-2022

[GITH2022b] - Github Project OpenSSL
https://github.com/openssl/openssl

[OPEN2022a] - OpenSSL Projekt
https://www.openssl.org/

[OPEN2022b] - Security Policy
https://www.openssl.org/policies/general/security-policy.html

[OPEN2022c] - Forthcoming OpenSSL Releases
https://mta.openssl.org/pipermail/openssl-announce/2022-October/000238.html

Update 1:
[OPEN2022d] Advisory des OpenSSL-Projekts
https://www.openssl.org/news/secadv/20221101.txt

[OPEN2022e] FAQ des OpenSSL-Projekts zu den Schwachstellen
https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

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.