NFIR Threat Intelligence Report

Kritieke kwetsbaarheden in OpenSSL-softwarebibliotheek

Datum: 1/11/2022

Versie: 1.0

bsi ISO/IEC 27001 Information Security Management CERTIFIED

NFIR

Beschrijving

Op 25 oktober 2022 is er een vooraankondiging gepubliceerd[1] door het OpenSSL Project Team inzake een kwetsbaarheid met de door het OpenSSL Project Team gegeven classificatie “CRITICAL”.

Omdat de OpenSSL-softwarebibliotheek aanwezig is in veel verschillende software producten, zowel in commerciële als open source, is ervoor gekozen om een Threat Intelligence Report te publiceren.

Wat is OpenSSL?

OpenSSL is een software-bibliotheek die gebruikt wordt voor cryptografische doeleinden, vooral op het gebied van netwerkverbindingen. Webservers gebruiken OpenSSL bijvoorbeeld vaak om versleutelde HTTPS-verbindingen tot stand te brengen. Mailservers en VPN-protocollen zoals OpenVPN gebruiken ook OpenSSL om versleutelde communicatiekanalen tot stand te brengen. De bibliotheek is te vinden in een breed scala aan producten, waaronder netwerkapparatuur, embedded systemen en container images.

De getroffen producten betreffen volgens het OpenSSL Project team tenminste de volgende producten:

CVE-nummer	Product	Classificatie[2]
Onbekend	De kwetsbaarheid is aanwezig in producten die OpenSSL 3.0.0-3.0.6 gebruiken. Producten die OpenSSL 1.0.2 of 1.1.1 gebruiken zijn niet getroffen.	Kritiek

Tabel 1: Overzicht van de getroffen producten

Het Nederlandse Nationaal Cyber Security Centrum (NCSC-NL) is daarnaast actief bezig met het in kaart brengen van kwetsbare software-producten, een overzicht hiervan is beschikbaar via https://github.com/NCSC-NL/OpenSSL-2022.

Publieke exploits

Er zijn op het moment van schrijven **nog geen publieke** exploits beschikbaar voor de beschreven kwetsbaarheden. NFIR schat het risico op eventueel misbruik in de toekomst als **reëel** in.

Aanbeveling

Voor ontwikkelaars van applicaties die gebruik maken van OpenSSL, geldt het volgende advies:
Op 1 november 2022 is er (tussen 14.00 - 18.00) een update beschikbaar welke te downloaden is via het volgende (officiele) downloadkanaal:

- https://www.openssl.org/source/

Het advies is om tenminste te updaten naar OpenSSL versie 3.0.7. NFIR adviseert om, zodra de update beschikbaar is de update uit te voeren en deze vervolgens uit te rollen naar de betrokken systemen en applicaties.

> Voor applicaties van derden die u gebruikt, adviseert NFIR u om contact op te nemen met de leverancier voor eventuele updates.

[1] https://mta.openssl.org/pipermail/openssl-announce/2022-October/000238.html
[2] CVSS-classificatie op het moment van schrijven nog onbekend

Mogelijke Impact

Als een aanvaller in staat is om de kwetsbaarheid succesvol uit te buiten, dan kan dit, gegeven de tot nu toe bekende classificatie vanuit het OpenSSL Project Team, waarschijnlijk leiden tot hoge impact op de, confidentialiteit integriteit en beschikbaarheid (BIV).

Doordat het OpenSSL Project team ervoor heeft gekozen om een vooraankondiging te doen, is de volledige impact nog niet bekend.

> NFIR **adviseert** u om forensisch onderzoek te laten doen naar of uw systemen getroffen zijn.

Actieplan

Het is belangrijk voor uw organisatie om ten minste de volgende stappen te nemen:

1. Controleer (indien beschikbaar) de publiek beschikbare Indicators-of-Compromise (IoC's) op uw systemen om vast te stellen of er systemen mogelijk gecompromitteerd zijn, of laat extern preventief onderzoek uitvoeren naar uw systemen.
2. Breng in kaart waar OpenSSL in uw organisatie gebruikt wordt (als onderdeel van softwarepakketen of stand-alone) – gebruik hierbij de beschikbaar gestelde flowcharts op de website om vast te stellen welke kwetsbaarheden van toepassing zijn voor uw organisatie.
3. Bereid uw organisatie voor op de situatie dat er onverwacht patches uitgevoerd dienen te worden (buiten de reguliere update-timeframes) en pas patches gecontroleerd toe volgens de voor uw organisatie gebruikelijke procedure.
4. Voer de beschikbare beveiligingsupdates/patches, zodra deze gepubliceerd zijn, direct uit op de systemen en verifieer of de updates daadwerkelijk toegepast zijn. In het geval dat u een externe IT-dienstleverancier heeft: Laat uw leverancier deze handelingen uitvoeren en laat deze de handelingen en het resultaat hiervan schriftelijk aan u bevestigen.

Heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met zeer gevoelige of bijzondere persoonsgegevens)? Zo ja, heeft u mogelijk indicaties dat het systeem niet direct gemitigeerd en/of geüpdatet kan worden? Overweeg dan om het systeem tijdelijk uit te schakelen totdat deze geüpdatet kan worden.

Wat moet uw organisatie doen bij mogelijk misbruik?

Als uw organisatie vermoedelijk het slachtoffer is geworden van een aanval, is het dringende advies om onderzoek uit te laten voeren naar de toedracht, in hoeverre aanvallers mogelijk andere systemen hebben gecompromitteerd en welke informatie mogelijk ongeautoriseerd geraadpleegd is.

1. Koppel indien mogelijk de getroffen systemen los van het netwerk, maar laat deze aanstaan (in verband met eventuele sporen zoals het vluchtige geheugen – RAM);
2. Laat de getroffen systemen forensisch onderzoeken; zorg voor adequate back-ups;
3. Reset uw wachtwoorden en gebruikersgegevens;
4. Doe aangifte bij de Politie;
5. Overweeg een melding te doen bij de Autoriteit Persoonsgegevens.

Heeft uw organisatie op dit moment een incident? Onze Computer Emergency Response Teams (CERT) staan 24/7 voor organisaties klaar om te ondersteunen bij IT- Security Incidenten.

Bel dan 088 133 0700 en wij doen ons uiterste best om u zo snel mogelijk te helpen. (Meer informatie over onze Incident Response Dienst.)

Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: Hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

Gespecialiseerd in

- Het verzamelen, identificeren en valideren van digitale informatie
- Onderzoek naar computers, servers, e-mailverkeer, gegevensdragers, websites en personen

Multidisciplinair onderzoek

- Sporen en gegevens verzamelen en reconstrueren
- Heldere rapportage bruikbaar voor juridische procedures en andere officiële instanties

Samenwerking met

- Tactisch rechercheurs, privacy juristen, gerechtsdeurwaarders, Politie, NCSC, IBD, het Openbaar Ministerie en internationale diensten.

NFIR als adviseur Forensisch Onderzoek

- Samen met de opdrachtgever wordt de scope van het onderzoek bepaald
- Praktisch toepasbare adviezen na afronding van het onderzoek

NFIR B.V.
Verlengde Tolweg 2
2517 JV Den Haag
Telefoon: 088 - 323 02 05
info@nfir.nl
https://www.nfir.nl