NFIR Threat Intelligence Report

Nieuwe kwetsbaarheden in Apache Commons Text (CVE-2022-42889) – Text2Shell

Datum: 20/10/2022
Versie: 1.0

Beschrijving

Op 18/19 oktober 2022 is een blog gepubliceerd door GHSL[1]-researcher Alvaro Muñoz (@pwntester), dat kwetsbaarheden in Apache Commons Text zijn geconstateerd. Een fout in de Apache Commons Text-bibliotheek kan worden gebruikt om op afstand code uit te voeren.

Apache Commons Text is een populaire open-source Java-bibliotheek met een "interpolatiesysteem" waarmee ontwikkelaars tekenreeksen kunnen wijzigen, decoderen en genereren op basis van ingevoerde tekenreeksen.

De getroffen producten betreffen volgens Apache tenminste de volgende producten:

CVE-nummer	Product	CVSS-classificatie
CVE-2022-42889	Apache Commons Text • Versies voor 1.10.0	Kritiek (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Tabel 1: Overzicht van de getroffen producten

Publieke exploits

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

Aanbeveling

Voor ontwikkelaars van applicaties die gebruik maken van Apache Commons Text, geldt het volgende advies:

Er is een nieuwe versie beschikbaar welke te downloaden is via de URL:

- https://commons.apache.org/proper/commons-text/

NFIR adviseert om zo snel als mogelijk een upgrade 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.

Mogelijke Impact

Als een aanvaller in staat is om de kwetsbaarheid succesvol uit te buiten, dan kan dit leiden tot het uitvoeren van ongeautoriseerde code op de getroffen systemen. Dit kan mogelijk erin resulteren dat de server en de aanwezige data gecompromitteerd raakt. Deze aanval kan uitgevoerd worden vanaf het internet waarbij authenticatie vereist is.

Vanuit een gecompromitteerde server kan een aanvaller mogelijk toegang verkrijgen tot de machine en mogelijk tot de rest van het netwerk.

Voor diensten van derden die u gebruikt, adviseert NFIR u om contact op te nemen met de leverancier zodat, zodra de patches beschikbaar zijn, deze kunnen worden toegepast.

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

Actieplan

[1] https://securitylab.github.com/advisories/GHSL-2022-018_Apache_Commons_Text/

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

1. Controleer 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. Voer de beschikbaar gestelde workarounds uit om, waar mogelijk, de impact te beperken.
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