NFIR Threat Intelligence Report

Indicaties dat kwetsbaarheid Spring4Shell (CVE-2022-22965) mogelijk actief misbruikt wordt

Datum: 01/04/2022
Versie: 1.0

bsi ISO/IEC 27001 Information Security Management CERTIFIED

NFIR

Beschrijving

Spring Core Framework is een verzameling van Java-softwarebibliotheken die kunnen worden gebruikt in softwareprogramma's die in Java geschreven zijn. Spring Core is ingebakken in veel Java-software.

De kwetsbaarheid maakt het mogelijk dat een aanvaller - zonder vereiste authenticatie- in bepaalde omstandigheden ongeautoriseerde code kan uitvoeren en toegang kan krijgen tot het programma of de applicatie en de bijbehorende informatie. Om misbruik te kunnen maken van deze kwetsbaarheid, zijn er momenteel diverse technische randvoorwaarden bekend. Deze zijn hieronder opgesomd. Mogelijk is deze lijst momenteel nog niet volledig.

Voor zover duidelijk, is de applicatie kwetsbaar als deze voldoet aan de volgende voorwaarden:

- Maakt gebruik van Spring Core Framework (tot en met versie 5.3.17);
- Maakt gebruik van spring-webmvc of spring-webflux dependencies (onbevestigd);
- Maakt gebruik van form bindings met "name=value" data;
- Maakt geen gebruik van een allowlist of denylist waarbij het gebruik van specifieke velden wordt uitgesloten (zoals "class", "module" en "classLoader");
- Draait op Java-versie 9 (JDK) of hoger.

Kortom, applicaties die op afstand toegankelijk zijn, gebruikersinvoer kunnen verwerken en Spring Core Framework (een versie lager dan 5.3.17) gebruiken om deze invoer te verwerken, zijn mogelijk kwetsbaar.

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 resulteren in het compromitteren van de server waar de applicatie op draait. Deze aanval kan uitgevoerd worden vanaf het internet, zonder dat daar authenticatie voor nodig is.

Vanuit een gecompromitteerde server kan een aanvaller mogelijk toegang verkrijgen tot de rest van het netwerk. Om deze reden is de CVSS-score[2] van de kwetsbaarheid geclassificeerd als **kritiek** (9.8).

Indicaties misbruik

Op het moment van schrijven zijn er meerdere indicatoren dat er actief geprobeerd wordt om misbruik te maken van de kwetsbaarheid . Hieronder vallen pogingen tot het uitbuiten van de kwetsbaarheid door bekende malafide IP-adressen[3]

[1] Het is mogelijk dat later nog aanvullende voorwaarden bekend worden.

[2] https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H; https://tanzu.vmware.com/security/cve-2022-22965

[3] https://otx.alienvault.com/pulse/6246c5778ca27726b90d842e

Detectie

Doordat de kwetsbare functionaliteit zich in een populaire Java-softwarebibliotheek bevindt is de huidige scope of impact niet inzichtelijk. Het is zeer waarschijnlijk dat veel gebruikte applicaties kwetsbaar zijn. Van een aantal applicaties is momenteel nog niet bekend of zij vallen onder de kwetsbare categorie. Dit heeft als gevolg dat het detecteren van iedere vorm van misbruik een complexe zaak is.

Er is wel een scanner gepubliceerd die mogelijk de aanwezigheid van het Spring Framework (lokaal) op systemen kan detecteren – deze scanner is gepubliceerd via het code-platform GitHub:

- https://github.com/hillu/local-spring-vuln-scanner

Aanbeveling

Voor ontwikkelaars van applicaties die gebruik maken van Spring Framework, geldt het volgende advies:
Er is een nieuwe versie van Spring Framework beschikbaar die te downloaden is via de URL **Het advies is om tenminste te updaten naar** Spring Framework versie **5.3.18** (met Spring Boot **2.6.6** of **2.5.12**) of Spring Framework **5.2.20**.

NFIR adviseert om zo snel als mogelijk een upgrade uit te voeren en deze vervolgens uit te rollen naar de betrokken systemen en applicaties.

Op het moment dat upgraden niet mogelijk is, kunnen de volgende twee mitigaties toegepast worden:

1. Voor organisaties die Spring Framework zelf gebruiken en binnen applicaties specifieke bindings hebben die niet-standaard datatypes gebruiken, is het van belang om de toegestane velden die de applicatie mag gebruiken te specificeren. Meer informatie hierover is beschikbaar in de Spring Documentatie: https://docs.spring.io/spring-framework/docs/current/javadoc-api/org/springframework/validation/DataBinder.html#:~:text=fields%20when%20binding.-,setAllowedFields,-public%C2%A0void%C2%A0setAllowedFields
2. Een tweede beschikbare mitigatie (in het geval dat Tomcat gebruikt wordt als onderliggende webserver) betreft het updaten van Tomcat naar versie 10.0.20, 9.0.62, en 8.5.78 (of hoger) waarmee de aanvalsroute via Tomcat niet langer functioneert. Meer informatie hierover is beschikbaar op de website van Spring: https://spring.io/blog/2022/04/01/spring-framework-rce-mitigation-alternative

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

Actieplan

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

1. Breng in kaart welke individuele leveranciers u heeft voor on-premise softwarepakketten, Software-as-a-Service (SaaS) of andere applicatie-leveranciers;
2. Raadpleeg de website van uw leveranciers en stel vast of er een vorm van 'dependency-lijsten' beschikbaar zijn waarbinnen u kunt controleren of 'Spring Framework' gebruikt wordt binnen de applicatie;
3. Neem contact op met uw leveranciers om te verifiëren of er binnen de applicaties 'Spring Framework' gebruikt wordt en welke versie van Spring Framework er gebruikt wordt;
4. 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.

Heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met gevoelige of bijzonder persoonsgegevens)? Zo ja, heeft u mogelijk indicaties dat Java met Spring Framework gebruikt wordt en zijn er nog geen updates beschikbaar? Overweeg dan om het systeem tijdelijk uit te schakelen.

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, de mate waarin 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. Dit in verband met eventuele sporen zoals het vluchtige geheugen – RAM;
2. Laat de getroffen systemen forensisch onderzoeken en 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.

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