# 0day kwetsbaarheid verholpen in Spring Core Framework

> Deze pagina gebruikt slimmigheden om officiële advisory platte tekst naar HTML om te zetten. Daarbij kan die informatie worden verminkt. De "Signed-PGP" versies waarnaar verwezen wordt zijn normatief (maar deze zijn minder leesbaar).

| Publicatie | Kans | Schade | | |
|---|---|---|---|---|
| | **Versie 1.03** | **01-04-2022** | **NCSC-2022-0221** | |
| | high | high | Signed-PGP → | |
| 01-04-2022 | high | high | NCSC-2022-0221 [1.03] | Signed-PGP → |

Kenmerken

## Kenmerken

- (Remote) code execution (Administrator/Root rechten)
- Toegang tot gevoelige gegevens

Omschrijving

## Omschrijving

Er is een kwetsbaarheid ontdekt in Spring Core Framework. Spring Core Framework is een set van Java libraries waarmee op gestructureerde wijze applicaties kunnen worden ontwikkeld die vervolgens zowel standalone kunnen draaien of in webapplicatie-omgevingen als Tomcat.

Een kwaadwillende kan de kwetsbaarheid misbruiken om willekeurige code uit te voeren in de scope van de ontwikkelde applicatie, en mogelijk daarmee toegang kan krijgen tot gevoelige informatie binnen die applicatie. Omdat niet valt vast te stellen met welke rechten de applicatie actief is, kan misbruik van deze kwetsbaarheid mogelijk leiden tot de uitvoer van willekeurige code met verhoogde rechten op het onderliggende systeem.

Voor deze kwetsbaarheid is nog geen CVE-kenmerk bekend gesteld. Om onderscheid te maken heeft deze kwetsbaarheid de naam "Spring4Shell" gekregen.

Deze kwetsbaarheid is een andere dan de kwetsbaarheid in Spring Cloud Function (CVE-2022-22963) waarvoor het NCSC beveiligingsadvies NCSC-2022-0220 heeft uitgebracht. Doordat beide kwetsbaarheden zeer kort op elkaar zijn gepubliceerd, is hier veel verwarring over ontstaan.

Inmiddels is Proof-of-Concept code verschenen waarmee de kwetsbaarheid kan worden aangetoond, maar nog niet misbruikt. Er worden echter (nog onbevestigde) meldingen gemaakt dat er pogingen

| Publicatie | Kans | Schade |
|---|---|---|

worden ondernomen om deze kwetsbaarheid actief te misbruiken. Vooralsnog zijn nog geen geslaagde pogingen waargenomen. Dit heeft vooral te maken met het feit dat er aan diverse randvoorwaarden moet worden voldaan, zoals JDK versie 9 of hoger, het gebruiken van Spring Beans, Spring Parameter Binding en die binding moet geconfigureerd zijn om van niet standaard types als POJO gebruik te maken.

Bereik

## Bereik

| Platforms | Producten | Versies |
|---|---|---|
| | Spring Framework | < 5.2.20 < 5.3.18 |

Oplossingen

## Oplossingen

## Spring.io

Spring.io heeft updates beschikbaar gesteld om de kwetsbaarheid te verhelpen in Spring Framework versie 5.3.18 en 5.2.20. Voor meer informatie zie [Link]

Ook zijn diverse mitigerende maatregelen gepubliceerd door beveiligingsonderzoekers. De mitigerende maatregelen die op dit moment beschikbaar zijn gesteld vereisen aanpassingen aan de code van de getroffen applicatie.

Zo kan een aanval, die in een serie van stappen moet worden uitgevoerd, worden gestopt door blacklisting toe te passen op de functie DataBinder. Informatie hierover kan worden verkregen via onderstaande link [Link]

Extra achtergrondinformatie, en methodes om te bepalen of een applicatie kwetsbaar is, vindt u op onderstaande link [Link]

Het NCSC houdt de ontwikkelingen in de gaten en heeft een publieke GitHub-pagina geopend waarin de ontwikkelingen rond de kwetsbaarheid actueel wordt bijgewerkt zodra informatie beschikbaar komt en bevestigd kan worden. Op deze GitHub is ook een lijst met software te vinden waarvan bekend is geworden dat ze ontwikkeld is met behulp van Spring Framework, of en zo ja hoe ze kwetsbaar is voor deze kwetsbaarheid en of er updates beschikbaar zijn of komen. Deze GitHub-pagina kunt u vinden op onderstaande link [Link]

CVE's

## CVE's

CVE-2022-22965

Kans

## Kans

Onderstaande tabel geeft in detail aan hoe wij tot de inschatting zijn gekomen hoe groot de kans is dat deze kwetsbaarheid in het doorsnee praktijkgeval kan worden misbruikt. De punten worden bij elkaar geteld.

| Publicatie | Kans | Schade |
|---|---|---|

| | ● high | Σ = 29 |
|---|---|---|
| Is de kwetsbaarheid aanwezig in de standaard configuratie/ installatie? | Nee | 1 |
| Is er exploit-code beschikbaar? | Proof of Concept (PoC) | 4 |
| Wordt de kwetsbaarheid in de praktijk gebruikt? | Beperkt waargenomen | 2 |
| Zijn er technische details beschikbaar? | Beperkt | 2 |
| Welke toegang is er nodig? | Internet | 6 |
| Vereiste credentials | Geen | 4 |
| Hoe moeilijk is het om de kwetsbaarheid uit te buiten? | Complex | 1 |
| Is er gebruikers interactie nodig? | Geen handelingen | 4 |
| Wordt misbruik of een exploit verwacht? | Ja binnenkort | 3 |
| Is er een oplossing beschikbaar? | Korter dan twee maanden | 2 |

Schade

## Schade

Onderstaande tabel geeft in detail aan hoe wij tot de inschatting zijn gekomen voor de schade die bij een succesvolle aanval kan ontstaan. De hoogste inschaling bepaalt de totale kans op schade.

| | | ● high |
|---|---|---|
| Denial of Service | Nee | ● low |
| Uitvoeren van willekeurige code | Ja, Root/Administrator-rechten | ● high |
| Rechten op afstand (remote [root-] shell) | Nee | ● low |
| Verwerven lokale admin/root-rechten (privilege escalation) | Nee | ● low |

| Publicatie | Kans | Schade | | |
|---|---|---|---|---|
| | | | | high |
| | | Lekken van (gevoelige) informatie | Ja, Gebruikersdata | high |
| | **Versie 1.03** | **01-04-2022** | **NCSC-2022-0221** | |
| | high | high | Signed-PGP → | |
| 01-04-2022 | high | high | NCSC-2022-0221 [1.03] | Signed-PGP → |
| Update | **Update**<br>Er is een CVE-kenmerk toegekend aan de kwetsbaarheid: CVE-2022-22965.<br><br>Het NCSC heeft een publieke GitHub-pagina geopend, waarin bijgehouden wordt van welke software bekend is dat ze ontwikkeld is met behulp van Spring Framework en in hoeverre de kwetsbaarheid aanwezig is. Hierin wordt bijgehouden wanneer updates beschikbaar zijn zodra die informatie bekend wordt. | | | |
| | **Versie 1.02** | **31-03-2022** | **NCSC-2022-0221** | |
| | high | high | Signed-PGP → | |
| 31-03-2022 | high | high | NCSC-2022-0221 [1.02] | Signed-PGP → |
| Update | **Update**<br>Spring.io heeft updates beschikbaar gesteld die de kwetsbaarheid verhelpen. | | | |
| | **Versie 1.01** | **31-03-2022** | **NCSC-2022-0221** | |
| | high | high | Signed-PGP → | |
| 31-03-2022 | high | high | NCSC-2022-0221 [1.01] | Signed-PGP → |

| Publicatie | Kans | Schade | | |
|---|---|---|---|---|
| Update | **Update**<br>Er is aanvullende informatie gepubliceerd waarmee kan worden bepaald of een applicatie kwetsbaar is. De link naar de onderzoekers is toegevoegd in "Mogelijke oplossingen" | | | |
| | **Versie 1.00** | **31-03-2022** | **NCSC-2022-0221** | |
| | high | high | Signed-PGP → | |
| 31-03-2022 | high | high | NCSC-2022-0221 [1.00] | Signed-PGP → |

## Vrijwaringsverklaring

Door gebruik van deze security advisory gaat u akkoord met de navolgende voorwaarden. Ondanks dat het NCSC de grootst mogelijke zorg heeft betracht bij de samenstelling van dit beveiligingsadvies, kan het NCSC niet instaan voor de volledigheid, juistheid of (voortdurende) actualiteit van dit beveiligingsadvies. De informatie in dit beveiligingsadvies is uitsluitend bedoeld als algemene informatie voor professionele partijen. Aan de informatie in dit beveiligingsadvies kunnen geen rechten worden ontleend.
Het NCSC en de Staat zijn niet aansprakelijk voor enige schade ten gevolge van het gebruik of de onmogelijkheid van het gebruik van dit beveiligingsadvies, waaronder begrepen schade ten gevolge van de onjuistheid of onvolledigheid van de informatie in dit beveiligingsadvies.
Op dit beveiligingsadvies is Nederlands recht van toepassing. Alle geschillen in verband met en/of voortvloeiend uit dit beveiligingsadvies zullen worden voorgelegd aan de exclusief bevoegde rechter te Den Haag. Deze rechtskeuze geldt tevens voor de voorzieningenrechter in kort geding.