NFIR Threat Intelligence Report

Patches beschikbaar voor actief misbruikte kritieke kwetsbaarheid in WSO2

Datum: 25/04/2022
Versie: 1.0

Beschrijving

Op dinsdag 25 april 2022 heeft het Nederlandse Nationaal Cyber Security Centrum (NCSC) een beveiligingsadvies gepubliceerd naar aanleiding van gepubliceerde beveiligingspatches voor de producten[1] van WSO2. Daarnaast is actief misbruik van de kwetsbaarheid in het wild waargenomen.

WSO2 is een leverancier van open-source technologie, opgericht in 2005. Het biedt een enterprise platform voor de integratie van application programming interfaces (API's), applicaties en webservices lokaal en over het Internet.

De specifieke kwetsbaarheid waarvoor dit Threat Intelligence Report geschreven is betreft CVE-2022-29464 waarmee het voor een aanvaller mogelijk is om zonder te authentiseren een achterdeur te plaatsen op het getroffen systeem.

De getroffen producten betreffen volgens WSO2 tenminste de volgende producten:

CVE-nummer	Product	CVSS3.1-score
CVE-2022-29464	WSO2 API Manager 2.2.0 en hoger WSO2 Identity Server 5.2.0 en hoger WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, 5.6.0 WSO2 Identity Server as Key Manager 5.3.0 en hoger WSO2 Enterprise Integrator 6.2.0 en hoger	9.8

Tabel 1: Overzicht van de getroffen producten

Gezien de ernst van deze kwetsbaarheden adviseert NFIR om de beschikbaar gestelde patches zo snel mogelijk te installeren.

Publieke exploits

Er zijn **publieke** exploits beschikbaar voor de beschreven kwetsbaarheid. Mede doordat deze kwetsbaarheden voor aanvallers zeer relevant zijn om toegang te kunnen verkrijgen tot systemen, schat NFIR het risico op eventueel misbruik als **zeer reëel** in.

Inmiddels zijn er verschillende meldingen online van gehackte systemen waarop crypto-miners of anders malafide software geïnstalleerd gebruikmakend van deze kwetsbaarheid.

> Onderzoekers van NFIR hebben de functionele werking van enkele gepubliceerde exploits voor CVE-2022-29464 onderzocht en heeft **bevestigd** dat de exploits zouden kunnen leiden tot ongeautoriseerde toegang.

[1] https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738

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 geen authenticatie vereist 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 kwetsbaarheden geclassificeerd als kritiek (9.8).

Legenda CVSS-scores

Classificatie	Score
Kritiek	9.0 – 10.0
Hoog	7.0 – 8.9
Gemiddeld	4.0 – 6.9
Laag	0.1 – 3.9
Informatief	0.0

Tabel 2: CVSS-scores

[2] https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738

Aanbeveling

NFIR adviseert om zo snel als mogelijk de betrokken systemen te voorzien van de door WSO2 beschikbaar gestelde beveiligingsupdates:

- https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738

Op het moment dat het toepassen van de beveiligingsupdates (nu) niet mogelijk is, kunnen de volgende mitigaties toegepast worden:

Productversie	Tijdelijk mitigatie
WSO2 API Manager 2.6.0, 2.5.0, 2.2.0 en oudere versies WSO2 Identity Server 5.8.0, 5.7.0, 5.6.0, 5.5.0, 5.4.1, 5.4.0, 5.3.0, 5.2.0 en oudere versies WSO2 Identity Server as Key Manager 5.7.0, 5.6.0, 5.5.0, 5.3.0 en oudere versies WSO2 IS Analytics 5.6.0, 5.5.0, 5.4.1, 5.4.0 en oudere versies	Verwijder alle vewijzingen in de **FileUploadConfig** tag in <product_home>/repository/conf/carbon.xml

WSO2 API Manager 4.0.0, 3.2.0, 3.1.0, 3.0.0	Voeg de volgende configuratie toe aan <product_home>/repository/conf/deployment.toml:
	`[[resource.access_control]]`
	`context="(.*)/fileupload/resource(.*)"`
	`secure=false`
	`http_method = "all"`
	
	`[[resource.access_control]]`
	`context="(.*)/fileupload/(.*)"`
	`secure=true`
	`http_method = "all"`
	`permissions = ["/permission/protected/"]`

WSO2 Identity Server 5.11.0, 5.10.0, 5.9.0
 	
WSO2 Identity Server / Key Manager 5.10.0, 5.9.0
	Voeg de volgende configuratie toe aan <product_home>/repository/conf/deployment.toml:
	`[[resource.access_control]]`
	`context="(.*)/fileupload/service(.*)"`
	`secure=false`
	`http_method = "all"`
	
	`[[resource.access_control]]`
	`context="(.*)/fileupload/entitlement-policy(.*)"`
	`secure=false`
	`http_method = "all"`
	
	`[[resource.access_control]]`
	`context="(.*)/fileupload/resource(.*)"`
	`secure=false`
	`http_method = "all"`
	
	`[[resource.access_control]]`
	`context="(.*)/fileupload/(.*)"`
	`secure=true`
	`http_method = "all"`
	`permissions = ["/permission/protected/"]`

WSO2 Enterprise Integrator 6.6.0, 6.5.0, 6.4.0, 6.3.0, 6.2.0, en oudere versies	Voor het EI-profiel dienen de onderstaande verwijzingen binnen het in het <product_home>/conf/carbon.xml bestand in de <FileUploadConfig> sectie van het

	XML-bestand te worden verwijderd.
	Dezelfde wijzigingen dienen te worden toegepast voor de Business process/ Broker en Analytics in de carbon.xml-bestanden op de volgende locaties:
	• <product_home>/wso2/broker/conf/carbon.xml
	• <product_home>/wso2/business-process/conf/carbon.xml
	• <product_home>/wso2/analytics/conf/carbon.xml
	`<Mapping>`
	`  <Actions>`
	`  <Action>keystore</Action>`
	`  <Action>certificate</Action>`
	`  <Action>*</Action>`
	`  </Actions>`
	`  <Class>org.wso2.carbon.ui.transports.fileupload.AnyFileUploadExecutor</Class>`
	`</Mapping>`
	
	`<Mapping>`
	`  <Actions>`
	`  <Action>jarZip</Action>`
	`  </Actions>`
	`  <Class>org.wso2.carbon.ui.transports.fileupload.JarZipUploadExecutor</Class>`
	`</Mapping>`
	
	`<Mapping>`
	`  <Actions>`
	`  <Action>tools</Action>`
	`  </Actions>`
	
	`<Class>org.wso2.carbon.ui.transports.fileupload.ToolsFileUploadExecutor</Class>`
	`</Mapping>`
	
	`<Mapping>`
	`  <Actions>`
	`  <Action>toolsAny</Action>`
	`  </Actions>`
	
	`<Class>org.wso2.carbon.ui.transports.fileupload.ToolsAnyFileUploadExecutor</Class>`
	`</Mapping>`

Andere niet-ondersteunde producten/versies gebaseerd op WSO2 Carbon Kernel 4 versies	Verwijder alle verwijzingen gedefinieerd in de FileUploadConfig tag in <product_home>/repository/conf/carbon.xml

Voor diensten van derden die u gebruikt, adviseert NFIR u om contact op te nemen met de leverancier voor de bevestiging dat eventuele updates toegepast zijn.

Actieplan

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

1. 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.
2. Voer de beschikbare beveiligingsupdates/patches uit op de systemen en verifieer of de updates daadwerkelijk toegepast zijn - In het geval van externe IT-dienstleverancier: Laat uw leverancier deze handelingen uitvoeren en laat deze handelingen en het resultaat hiervan schriftelijk aan u bevestigen.

> Heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met gevoelige of bijzonder persoonsgegevens)? Zo ja heeft u mogelijk indicaties dat het systeem niet direct 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