NFIR Threat Intelligence Report

Actief misbruikte kwetsbaarheid in Confluence laat aanvallers ongeautoriseerde code uitvoeren (CVE-2022-26134)

Datum: 03/06/2022
Versie: 1.0

Beschrijving

Op 2 en 3 juni 2022 is informatie gepubliceerd over een kwetsbaarheid in Confluence producten van Atlassian, waarmee aanvallers volledige toegang kunnen krijgen tot machines en mogelijk achterliggende netwerkcomponenten. Confluence wordt door organisaties onder andere gebruikt als web-gebaseerde wiki- en informatieplatform.

De specifieke kwetsbaarheid waarvoor dit Threat Intelligence Report geschreven is betreft CVE-2022-26134. Door de kwetsbaarheid is het voor een aanvaller mogelijk is om zonder te authentiseren toegang te verkrijgen, waarna malafide code uitgevoerd kan worden op het getroffen systeem.

De getroffen producten betreffen volgens Atlassian tenminste de volgende producten:

CVE-nummer	Product	CVSS3.1-score[1]
CVE-2022-26134	Confluence – Alle versies • Confluence Server • Confluence Data Center	9.8

Tabel 1: Overzicht van de getroffen producten

> Op het moment van schrijven zijn volgens Atlassian alle versies[2] van Confluence **kwetsbaar** en zijn er nog geen patches gepubliceerd.

Confluence stelt daarnaast dat Atlassian Cloud-hosted instances niet kwetsbaar lijken en dat er geen actieve aanvalspogingen zijn waargenomen naar Atlassian Cloud-hosted instances. Het is echter van belang om alert te blijven en updates die gepubliceerd worden te blijven volgen.

Publieke exploits

Er zijn op het moment van schrijven **nog geen publieke** exploits beschikbaar voor de beschreven kwetsbaarheid. Echter is de verwachting dat deze op **zeer korte** termijn beschikbaar worden. Omdat 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.

[1] https://thehackernews.com/2022/06/hackers-exploiting-unpatched-critical.html
[2] https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

Mogelijke Impact

Als een aanvaller in staat is om de kwetsbaarheid succesvol uit te buiten, 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 machine en mogelijk tot de rest van het netwerk. Dit kan leiden tot het ontvreemden van (persoons)gegevens, ransomware of andere soorten malware. Om deze reden is de CVSS-score 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

Workarounds

Op het moment van schrijven zijn er geen patches gepubliceerd door Atlassian. Wel zijn er een aantal workarounds beschreven door Atlassian – u dient zelf te bepalen welke situatie voor uw organisatie van toepassing is:

- Optie 1: Koppel Confluence los van het internet (impact hiervan is dat Confluence niet langer via het internet benaderbaar is).
- Optie 2: Zorg ervoor dat Confluence enkel nog via een Virtual Private Network (VPN) benaderbaar is.
- Optie 3: Zorg ervoor dat Confluence enkel nog via een reverse-proxy beschikbaar is met pre-authenticatie.
- Optie 4: Zorg ervoor dat Confluence enkel via een Web Application Firewall (WAF) / Intrusion Prevention System (IPS) benaderbaar is en dat verbindingsverzoeken geblokkeerd worden die het volgende bevatten:

```
${
```

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.

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

Detectie

Een bekende methode om vast te stellen of malafide verbindingsverzoeken zijn binnengekomen op uw omgeving is hieronder per OS beschreven, onderverdeeld in Linux en Microsoft Windows.

Linux

Het volgende commando kan worden uitgevoerd om vast te stellen of de malafide karakters in logs aanwezig zijn van Confluence voor Linux systemen:

```
grep -a -i -e '${' <logging-locatie>/access.log
```

Microsoft Windows

Het volgende commando kan worden uitgevoerd om vast te stellen of de malafide karakters in logs aanwezig zijn van Confluence voor Windows systemen:

```
findstr -i "${" <installatie-map>/logs/*.access*.log
```

Actieplan

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

1. Controleer de publiek beschikbare Indicators-of-Compromise (IoCs) op uw systemen om vast te stellen of u mogelijk gecompromitteerd bent. Of laat extern preventief onderzoek uitvoeren naar uw systemen.
2. Voer eventueel beschikbaar gestelde work-arounds 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 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 aan staan (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 - https://www.nfir.nl/incident-response/)

Disclaimer: NFIR heeft er alles aan gedaan om deze informatie accuraat en betrouwbaar te maken. De verstrekte informatie is echter zonder enige garantie van welke aard dan ook en het gebruik ervan is geheel voor risico van de gebruiker. NFIR aanvaardt geen enkele verantwoordelijkheid of aansprakelijkheid voor de juistheid, de inhoud, de volledigheid, de rechtmatigheid of de betrouwbaarheid van de verstrekte informatie.

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