NFIR Threat Intelligence Report

Actief misbruikte kwetsbaarheid in BIG-IP F5 Firewall laat aanvallers ongeautoriseerde code uitvoeren (CVE-2022-1388)

Datum: 11/05/2022
Versie: 1.0

Beschrijving

Op 9 mei 2022 is aanvullende informatie gepubliceerd over een kwetsbaarheid in de iControl REST API van de BIG-IP firewall producten van F5, waarmee aanvallers volledige toegang kunnen krijgen tot de firewall en achterliggende netwerkcomponenten. Deze kwetsbaarheid betreft CVE-2022-1388 en stelt een aanvaller in staat om, zonder te authentiseren, op het hoogste niveau (root) code uit te voeren op het getroffen systeem.

Volgens F5 zijn de volgende producten getroffen:

CVE-nummer	Product		CVSS3.1-score
CVE-2022-1388	BIG-IP (alle modules)		9.8
	Versie 16.1.0 t/m 16.1.2	Opgelost in versie 16.1.2.2	
	Versie 15.1.0 t/m 15.1.5	Opgelost in versie 15.1.5.1	
	Versie 14.1.0 t/m 14.1.4	Opgelost in versie 14.1.4.6	
	Versie 13.1.0 t/m 13.1.4	Opgelost in versie 13.1.5	
	Versie 12.1.0 t/m 12.1.6	Zal niet worden opgelost	
	Versie 11.6.1 t/m 11.6.5	Zal niet worden opgelost	

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 hierboven beschreven kwetsbaarheid. Mede doordat deze kwetsbaarheid voor aanvallers zeer relevant is om toegang te kunnen verkrijgen tot systemen, schat NFIR het risico op eventueel misbruik als **zeer reëel** in.

> Onderzoekers van NFIR hebben de functionele werking van enkele gepubliceerde exploits voor CVE-2022-1388 onderzocht en hebben bevestigd dat de exploits (al dan niet in aangepaste vorm) zouden kunnen leiden tot ongeautoriseerde toegang op het hoogste niveau.

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. Hierdoor kan de aanwezige data op de server gecompromitteerd raken. De aanval kan uitgevoerd worden vanaf het internet waarbij geen authenticatie is vereist.

Vanuit een gecompromitteerde server kan een aanvaller mogelijk toegang verkrijgen tot de rest van het netwerk. Om deze reden is de CVSS-score[1] 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

Aanbeveling

NFIR adviseert om zo snel als mogelijk de betrokken systemen te voorzien van de door F5 beschikbaar gestelde beveiligingsupdates (account vereist):

- Versie 13 - https://downloads.f5.com/esd/product.jsp?sw=BIG-IP&pro=big-ip_v13.x
- Versie 14 - https://downloads.f5.com/esd/product.jsp?sw=BIG-IP&pro=big-ip_v14.x
- Versie 15 - https://downloads.f5.com/esd/product.jsp?sw=BIG-IP&pro=big-ip_v15.x
- Versie 16 - https://downloads.f5.com/esd/product.jsp?sw=BIG-IP&pro=big-ip_v16.x
- Versie 17 - https://downloads.f5.com/esd/product.jsp?sw=BIG-IP&pro=big-ip_v17.x

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

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

[1] https://support.f5.com/csp/article/K23605346

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 tot dat 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 of gestolen 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;
3. Zorg voor adequate back-ups;
4. Reset uw wachtwoorden en gebruikersgegevens;
5. Doe aangifte bij de Politie;
6. 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