NFIR Threat Intelligence Report

Fortinet Fortigate VPN-SSL-kwetsbaarheden (CVE-2023-27997)

Datum: 13/06/2022

Versie: 1.0

NFIR

Beschrijving

Op 12 juni 2023 heeft Fortiguard Labs[1] aangegeven meerdere kwetsbaarheden te hebben opgelost in meerdere versies van FortiOS. Eén van deze kwetsbaarheden, CVE-2023-27997[2] – ook wel Xortigate genoemd, betreft een heap-based buffer overflow kwetsbaarheid in FortiOS en FortiProxy SSL-VPN. Met deze kwetsbaarheid kan een aanvaller malafide code uitvoeren op het getroffen systemen. Door de ernst van de impact heeft het NCSC de ernst van de kwetsbaarheid[3] ingeschaald op **Hoog**/**Hoog**.

FortiOS is een netwerkbesturingssysteem voor next-generation firewalls (NGFW's), access-points, switches en Network Access Control (NAC)-oplossingen. FortiProxy is een webproxy die beschermt tegen aanvallen vanaf internet door meerdere detectietechnieken zoals web-filtering, DNS-filtering, preventie van gegevensverlies en antivirus. De getroffen versies van FortiOS/FortiProxy betreffen tenminste de volgende:

Product	Platform	CVSS-score
Tenminste - FortiOS-6K7K versie 7.0.10 - FortiOS-6K7K versie 7.0.5 - FortiOS-6K7K versie 6.4.12 - FortiOS-6K7K versie 6.4.10 - FortiOS-6K7K versie 6.4.8 - FortiOS-6K7K versie 6.4.6 - FortiOS-6K7K versie 6.4.2 - FortiOS-6K7K versie 6.2.9 t/m 6.2.13 - FortiOS-6K7K versie 6.2.6 t/m 6.2.7 - FortiOS-6K7K versie 6.2.4 - FortiOS-6K7K versie 6.0.12 t/m 6.0.16 - FortiOS-6K7K versie 6.0.10	FortiOS	9.8 – Kritiek
Tenminste - FortiProxy versie 7.2.0 t/m 7.2.3 - FortiProxy versie 7.0.0 t/m 7.0.9 - FortiProxy versie 2.0.0 t/m 2.0.12 - FortiProxy 1.2 alle versies - FortiProxy 1.1 alle versies	FortiProxy	9.8 – Kritiek
Tenminste - FortiOS versie 7.2.0 t/m 7.2.4 - FortiOS versie 7.0.0 t/m 7.0.11 - FortiOS versie 6.4.0 t/m 6.4.12 - FortiOS versie 6.2.0 t/m 6.2.13 - FortiOS versie 6.0.0 t/m 6.0.16	FortiOS	9.8 – Kritiek

Tabel 1: Overzicht van de getroffen producten

NFIR adviseert om vast te stellen of de kwetsbare versies van FortiOS/FortiProxy zoals hierboven beschreven aanwezig zijn op systemen binnen uw organisatie. Indien u een kwetsbare versie constateert, adviseert NFIR om incident response & digitaal forensisch onderzoek uit te laten voeren om te achterhalen of er sporen van misbruik van de kwetsbaarheid zijn.

> Acuut hulp nodig? Bel dan onze 24/7 CERT-lijn via **088 133 0700** en wij doen ons uiterste best om u zo snel mogelijk te helpen.

[1] https://www.fortiguard.com/psirt/FG-IR-23-097
[2] https://nvd.nist.gov/vuln/detail/CVE-2023-27997
[3] https://www.ncsc.nl/actueel/advisory?id=NCSC-2023-0282

Updates

Door Fortiguard Labs zijn de volgende versies van FortiOS/FortiProxy gepubliceerd welke niet langer kwetsbaar zijn voor CVE-2023-27997:

Product	Platform
- FortiOS-6K7K versie 7.0.12 of hoger - FortiOS-6K7K versie 6.4.13 of hoger - FortiOS-6K7K versie 6.2.15 of hoger - FortiOS-6K7K versie 6.0.17 of hoger	FortiOS
- FortiProxy versie 7.2.4 of hoger - FortiProxy versie 7.0.10 of hoger	FortiProxy
- FortiOS versie 7.4.0 of hoger - FortiOS versie 7.2.5 of hoger - FortiOS versie 7.0.12 of hoger - FortiOS versie 6.4.13 of hoger - FortiOS versie 6.2.14 of hoger - FortiOS versie 6.0.17 of hoger	FortiOS

Tabel 2 - FortiOS/FortiProxy update-versies

Actieplan

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

1. Indien uw organisatie gebruikmaakt van FortiGate/FortiProxy adviseert NFIR om vast te stellen of uw systemen kwetsbaar zijn. Controleer hiervoor de FortiOS/FortiProxy-versie van de aanwezige systemen binnen uw netwerkomgeving;
2. Indien er indicaties zijn dat uw systemen kwetsbaar zijn adviseert NFIR om forensisch onderzoek uit te laten voeren om vast te stellen of uw omgeving gecompromitteerd is.
3. Indien uw systemen kwetsbaar zijn adviseert NFIR om de getroffen systemen te updaten naar versies welke niet langer kwetsbaar zijn;
4. Controleer (indien beschikbaar) publiek beschikbare Indicators-of-Compromise (IoC's) op uw systemen om vast te stellen of er systemen mogelijk gecompromitteerd zijn, of laat extern preventief onderzoek uitvoeren naar uw systemen;

Zijn uw systemen kwetsbaar en heeft u systemen waarvan het risico groot is (bijvoorbeeld systemen met zeer gevoelige of bijzondere persoonsgegevens)? Zo ja, heeft u mogelijk indicaties dat het systeem niet direct gemitigeerd en/of geüpdatet kan worden? Overweeg dan om het systeem tijdelijk uit te schakelen totdat deze geüpdatet kan worden.

Wat moet mijn organisatie doen als zij getroffen is?

Als uw organisatie vermoedelijk slachtoffer is geworden van een aanval middels deze kwetsbaarheid, is het dringende advies om onderzoek uit te laten voeren naar de toedracht van het incident, 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;
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.

> Acuut hulp nodig? Bel dan onze 24/7 CERT-lijn via 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, incident responders die u helpen om aanvallen te mitigeren 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