ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de vulnerabilitat

CVE 2023-27997

TLP: WHITE

18/07/2023

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD		

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGÍA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar **TLP:AMBER** quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com **TLP:AMBER** únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar **TLP:GREEN** quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar **TLP:WHITE** quan la informació no suposa cap risc de mal ús, dins de les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de Copyright.

2. INTRODUCCIÓ

El present informe té com a objectiu donar a conèixer la vulnerabilitat que afecta la funcionalitat SSL VPN dels tallafocs Fortigate. Aquesta ha estat catalogada com CVE-2023-27997 i té un nivell de perillositat crític. Així mateix, pretenem que serveixi perquè les organitzacions que utilitzen aquests dispositius prenguin mesures proactives per mitigar el risc i protegir les seves infraestructures de xarxa.

Els tallafocs Fortigate, també coneguts com a firewalls de pròxima generació NGFW (Next-generation firewall), són dispositius de seguretat de xarxa que permeten la creació de xarxes segures i tenen com a objectiu la protecció enfront d'amenaces emergents i sofisticades. Aquests dispositius realitzen funcions de seguretat com tallafocs, detecció d'intrusions, filtrat web i protecció contra programari maliciós o correus no desitjats.

La vulnerabilitat CVE-2023-27997 representa una seriosa amenaça per a la seguretat dels firewalls de FortiGate, amb una alarmant quantitat de dispositius vulnerables, malgrat que fa un mes Fortinet publiqués una actualització que, suposadament, solucionava el problema. L'explotació d'aquesta vulnerabilitat podria tenir greus conseqüències per les organitzacions afectades, incloent-hi l'exposició d'informació confidencial i la pèrdua de control sobre els seus sistemes crítics.

En l'informe explicarem els antecedents, les característiques de la vulnerabilitat, els requisits d'explotació, l'impacte i el risc, com mitigar la vulnerabilitat així com una sèrie de recomanacions que seran útils per qualsevol tipus d'organització.

És fonamental que les organitzacions prenguin mesures immediates per protegir-se i aplacar el risc associat amb aquesta vulnerabilitat crítica. La seguretat de la xarxa i la protecció de les dades delicades han de ser prioritats per qualsevol mena d'organització.

3. ANTECEDENTS

L'11 de gener del 2023 l'empresa Fortinet va revelar l'incident FG-ANAR-22-398 / CVE-2022-42475, en el qual es va descobrir i es va explotar una porta del darrere basada en SSL VPN de FortiOS (el sistema operatiu de Fortinet). Després d'aquest incident, el PSIRT (equip de resposta a incidents de seguretat de productes de Fortinet), va iniciar una auditoria del codi del mòdul SSL-VPN amb la finalitat de garantir la seguretat i la integritat del producte.

Així mateix, el passat 9 de juny Fortinet va publicar noves actualitzacions de microprogramari que corregien una vulnerabilitat crítica que encara no havia estat divulgada. Aquestes correccions de seguretat es van publicar en les versions de microprogramari FortiOS 6.0.17, 6.2.15, 6.4.13, 7.0.12 i 7.2.5. Les noves versions incloïen comprovacions d'integritat del sistema que impedirien l'inici del dispositiu en cas de trobar-se compromès. Cal ressaltar que Fortinet és coneguda per llançar actualitzacions de seguretat abans de revelar les vulnerabilitats més crítiques, donant als clients temps per poder actualitzar els seus dispositius abans que els actors d'amenaces puguin actuar. Així i tot, a la pràctica això també pot donar avantatges als atacants.

L'11 de juny, l'investigador Charles Fol de la signatura francesa Lexfo, va donar a conèixer a través del seu compte de Twitter, que les noves actualitzacions estarien destinats a corregir la vulnerabilitat sota el CVE-2023-27997 que havia descobert al costat de Dany Bach (un altre investigador de la signatura). Segons aquesta recerca, les actualitzacions de seguretat haurien de considerar-se com urgents pels administradors de sistemes Fortinet, per evitar costi el que costi que els ciberdelinqüents descobreixin aquests errors i comencin a explotar-los activament.

Il·lustració 1: Captura del tuit publicat per Charles Fol.

El dilluns 12 juny Fortinet va llançar un avís de PSIRT crític de CVSS (FG-ANAR-23-097 / CVE-2023-27997) juntament amb altres correccions relacionades amb SSL-VPN. Cal destacar que FG-ANAR-23-097 correspon a l'ID de l'incident.

El 13 de juny Fortinet va publicar un nou avís en el qual s'informava que la vulnerabilitat CVE-2023-27997 podria haver estat explotada en atacs dirigits contra organitzacions governamentals, industrials i infraestructures crítiques. L'empresa també va comunicar que, després de la seva recerca sobre l'error de seguretat FG-ANAR-23-097, aquest podria haver estat

explotat en un nombre limitat de casos i que estaven treballant en estreta col·laboració amb els clients per monitorar la situació.

ID de l'incident	CVE NVD	Producte	Gravetat	Descripció
FG-IR-23-097	CVE-2023-27997	FortiOS	9.2 (Crític)	Desbordament del búfer d'emmagatzematge dinàmic en l'autenticació prèvia SSL-VPN
FG-IR-23-111	CVE-2023-29180	FortiOS	7.3 (Alt)	Eliminació de referència de punter nul en SSLVPNd
FG-IR-23-475	CVE-2023-22640	FortiOS	7.1 (Alt)	FortiOS: escriptura fora de límit a SSLVPNd
FG-IR-23-119	CVE-2023-29181	FortiOS	8.3 (Alt)	Error de format de cadena en el daemon Fcliense
FG-IR-23-125	CVE-2023-29179	FortiOS	6.4 (Mitjà)	Eliminació de referència de punter nul al punt final de proxy SSLVPNd
FG-IR-23-479	CVE-2023-22641	FortiOS	4.1 (Mitjà)	Obrir redirecció en SSLVPNd

Després d'haver explicat els antecedents i la cronologia de fets, passarem a explicar la vulnerabilitat.

4. LA VULNERABILITAT CVE 2023-27997

La vulnerabilitat, denominada CVE-2023-27997 (també coneguda com XORtigate), es refereix a una vulnerabilitat crítica de desbordament del búfer basada en el munt [CWE-122] a FortiOS i FortiProxy SSL-VPN que podria permetre que un atacant remot executi codi o ordres arbitràries a través de sol·licituds dissenyades específicament. Tal com hem esmentat, això posa en risc a un gran nombre d'organitzacions que confien en aquests dispositius per protegir les seves xarxes i dades més delicades.

Segons el Centre Criptològic Nacional, el CCN-CERT, i la signatura francesa de ciberseguretat Olympe Cyberdefense, aquesta vulnerabilitat permet a un atacant interferir a través d'una VPN, fins i tot si el MFA està activat.

4.1 Principals amenaces cibernètiques

La vulnerabilitat és una execució remot de codi amb una puntuació de gravetat de 9,8 sobre 10. A continuació, es detallaran les característiques principals d'aquesta vulnerabilitat:

Identificador	CVE-2023-27997
Data de publicació	13/06/2023
Software afectat	Fortinet Fortigate
Puntuació CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (9.8 Critical)
Nivell de gravetat	Crític
Vector d'atac	Network
Complexitat d'atac	Baix
Privilegis requerits	Cap
Interacció d'usuari	Cap
Abast	Sense alterar
Impacte en la confidencialitat	Alt
Impacte en la integritat	Alt
Impacte en la disponibilitat	Alt

A FortiOS versió 7.2.4 i anteriors, versió 7.0.11 i posteriors, versió 6.4.12 i posteriors, versió 6.0.16 i posteriors i FortiProxy versió 7.2.3 i posteriors, versió 7.0.9 i anteriors, versió 2.0.12 i posteriors, versió 1.2 totes les versions, versió 1.1 totes les versions SSL-VPN pot permetre que un atacant remot executi codi o ordres arbitràries a través de sol·licituds dissenyades específicament.

A tall de resum, les versions afectades són les següents:

- FortiOS-6K7K versió 7.0.10
- FortiOS-6K7K versió 7.0.5
- FortiOS-6K7K versió 6.4.12
- FortiOS-6K7K versió 6.4.10
- FortiOS-6K7K versió 6.4.8
- FortiOS-6K7K versió 6.4.6
- FortiOS-6K7K versió 6.4.2
- FortiOS-6K7K versió 6.2.9 a 6.2.13

- FortiOS-6K7K versió 6.2.6 a 6.2.7
- FortiOS-6K7K versió 6.2.4
- FortiOS-6K7K versió 6.0.12 a 6.0.16
- FortiOS-6K7K versió 6.0.10
- FortiProxy versió 7.2.0 a 7.2.3
- FortiProxy versió 7.0.0 a 7.0.9
- FortiProxy versió 2.0.0 a 2.0.12
- FortiProxy 1.2 totes les versions.
- FortiProxy 1.1 totes les versions.
- FortiOS versió 7.2.0 a 7.2.4
- FortiOS versió 7.0.0 a 7.0.11
- FortiOS versió 6.4.0 a 6.4.12
- FortiOS versió 6.2.0 a 6.2.13
- FortiOS versió 6.0.0 a 6.0.16

4.2 Detecció de la vulnerabilitat

La presència de la vulnerabilitat pot ser identificada mitjançant l'anàlisi de la versió actual de FortiOS. Aquesta informació pot ser accedida mitjançant la següent ordre a la consola de Fortinet Fortigate:

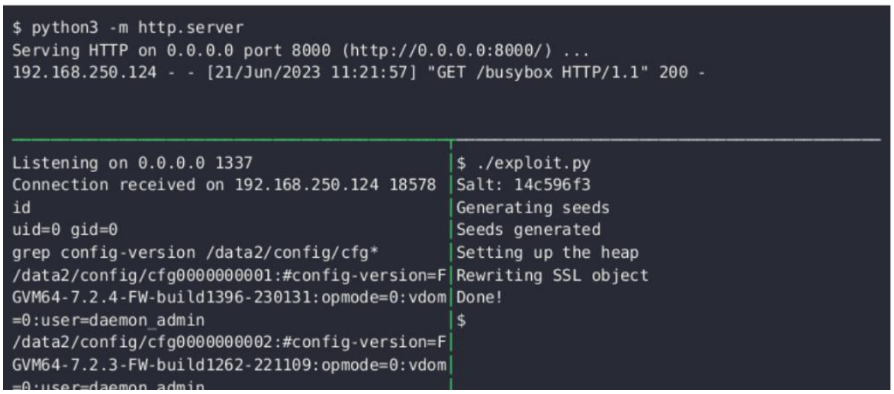
diagnose sys fortiguard-service status

Si la sortida del comando mostra FortiOS Versió 7.2.5, 7.0.12, 6.4.13, 6.2.15, o 6.0.17 o superiors, llavors el dispositiu no seria considerat vulnerable. Si la sortida mostrés un número de versió inferior, el dispositiu seria vulnerable i és necessari actualitzar-lo el més ràpid possible.

4.3 Requisits d'explotació

L'atacant ha de poder accedir al port configurat per les connexions VPN SSL del dispositiu.
La vulnerabilitat aprofita la possibilitat de redirigir el flux d'execució mitjançant l'enviament d'un contingut especialment preparat, l'amplitud del qual no és comprovada de manera adequada i així, corrompria la zona de memòria *heap* del dispositiu. Això permetria executar codi arbitrari o causar una denegació del servei, afectant de manera greu a la confidencialitat, integritat i disponibilitat del dispositiu.

L'equip de Bishop Fox va crear un *exploit* per a CVE-2023-27997. En la captura de pantalla següent es mostra *l'exploit* i com l'atacant es connecta de nou a un servidor controlat pel mateix, descàrrega un BusyBox binari i obre una *shell* interactiva.



Il·lustració 2: Codi d'execució remota a través de CVE 2023-27997 a FortiGate FGVM64 versió 7.2.4.

4.4 Impacte i risc

L'explotació efectuada amb èxit d'aquesta vulnerabilitat podria donar lloc a conseqüències devastadores, incloent-hi la filtració d'informació confidencial, el compromís de sistemes interns i la pèrdua de control sobre la infraestructura de xarxa.

Aquesta situació presenta un perill significatiu, ja que aquells que aconsegueixin explotar aquesta vulnerabilitat podrien comprometre la integritat de les defenses de seguretat, permetent el trànsit no autoritzat o fins i tot facilitant l'accés a altres sistemes interns.

Existeixen al voltant 490.000 interfícies VPN SSL exposades a Internet. El greu és que, segons les últimes avaluacions de seguretat, s'estima que aproximadament el 69% dels tallafocs de FortiGate estan en risc de ser explotats. Aquesta xifra alarmant destaca la necessitat immediata que les organitzacions que utilitzen aquests dispositius prenguin mesures proactives per mitigar el risc i protegir les seves infraestructures de xarxa.

Shodan revela que hi ha 250.000 tallafocs FortiGate exposats a Internet. Molts d'aquests articles usen la consulta ssl.cert.subject.cn:FortiGate, que busca qualsevol certificat SSL que s'hagi emès per FortiGate. No obstant això, aquesta consulta no filtra específicament les interfícies SSL VPN, que és on resideix aquesta vulnerabilitat. No troba dispositius amb certificats emesos per algú que no sigui Fortinet (per exemple, certificats autosignats, proxys inversos, etc.). Segons Shodan, al món existeixen al voltant de 564.750 instàncies Fortinet Fortigate potencialment vulnerables. A Iberoamèrica, el número ascendeix a 78.520 instàncies potencialment vulnerables.

4.5 Mitigació de la vulnerabilitat

La solució principal consisteix a actualitzar urgentment Fortinet Fortigate a les noves versions disponibles que corregeixen aquesta vulnerabilitat:

- FortiOS-6K7K versió 7.0.12 o superior.
- FortiOS-6K7K versió 6.4.13 o superior.
- FortiOS-6K7K versió 6.2.15 o superior.
- FortiOS-6K7K versió 6.0.17 o superior.
- FortiProxy versió 7.2.4 o superior.
- FortiProxy versió 7.0.10 o superior.
- FortiOS versió 7.4.0 o superior.
- FortiOS versió 7.2.5 o superior.
- FortiOS versió 7.0.12 o superior.
- FortiOS versió 6.4.13 o superior.
- FortiOS versió 6.2.14 o superior.
- FortiOS versió 6.0.17 o superior.

5. RECOMANACIONS

Els investigadors i experts en ciberseguretat insten les organitzacions que utilitzen els tallafocs de FortiGate al fet que adoptin mesures de manera immediata. Es recomana que les organitzacions verifiquin si els seus dispositius són vulnerables i apliquin les actualitzacions de seguretat corresponents proporcionades per Fortinet, el fabricant dels firewalls de FortiGate. A més, es recomana revisar les configuracions i polítiques de seguretat, així com implementar mesures addicionals de seguretat en capes per reforçar les defenses contra possibles atacs.

A més de la supervisió dels avisos de seguretat i l'aplicació immediata d'actualitzacions als sistemes, Fortinet recomana realitzar les següents accions:

- Minimitzar la superfície d'atac desactivant les funcions que no s'utilitzen i gestionar els dispositius a través d'un mètode fora de banda sempre que sigui possible.
- Revisar els seus sistemes a la recerca d'evidències d'explotació de vulnerabilitats anteriors, per exemple, FG-ANAR-22-377 / CVE-2022-40684.
- Mantenir una bona higiene cibernètica i seguir les recomanacions d'aplicació de pegats dels proveïdors.
- Seguir les recomanacions d'enduriment, per exemple, FortiOS 7.2.0 Hardening Guide.

6. GLOSSARI

CVE (Common Vulnerabilities and Exposures)

És una llista de vulnerabilitats i exposicions de seguretat de la informació divulgades públicament. CVE va ser llançat en 1999 per la corporació MITRE per a identificar i categoritzar vulnerabilitats en programari i microprogramari. CVE proporciona un diccionari gratuït perquè les organitzacions millorin la seva seguretat cibernètica. MITRE és una organització sense fins de lucre que opera centres de recerca i desenvolupament finançats amb fons federals als Estats Units.

Exploit

Un exploit és un programa informàtic, una part d'un programari o una seqüència de comandos que s'aprofita d'un error o vulnerabilitat per a provocar un comportament no intencionat o imprevist en un programari, maquinari o en qualsevol dispositiu electrònic. Aquests comportaments inclouen, en general, la presa del control d'un sistema, la concessió de privilegis d'administrador a l'intrús o el llançament d'un atac de denegació de servei (Dos o DDoS).

Firewall

Un firewall és una solució de seguretat de xarxes que protegeix la seva xarxa del trànsit no desitjat. Els firewalls o tallafocs bloquegen el programari maliciós entrant en funció d'un conjunt de regles prèviament programades. Aquestes regles també poden impedir que els usuaris dins de la xarxa accedeixin a determinats llocs i programes.

FortiOS

És el sistema operatiu que connecta tots els components de xarxa de Fortinet per integrar-los en la plataforma Security Fabric del proveïdor.

Fortiproxy

FortiProxy és un *proxy* web segur que protegeix els empleats contra els atacs que es transmeten per Internet mitjançant la incorporació de múltiples tècniques de detecció, com el Web Filtering, el DNS Filtering, la prevenció de pèrdua de dades, l'antivirus, la prevenció d'intrusions i la Advanced Threat Protection. FortiProxy ajuda a reduir les demandes d'amplada de banda i optimitza la xarxa amb emmagatzematge en caixet de contingut i vídeo. FortiProxy és un *proxy* d'alt rendiment amb appliances físics i virtuals que s'implementen en el lloc per donar servei a organitzacions de totes les grandàries.

Malware

És un tipus de programari que té com a objectiu danyar o infiltrar-se sense el consentiment del seu propietari en un sistema d'informació. Paraula que neix de la unió dels termes en anglès de programari malintencionat: malicious software. Dins d'aquesta definició té cabuda un ampli ventall de programes maliciosos: virus, cucs, troians, backdoors, spyware, etc. El punt en comú en tots aquests programes és el seu caràcter nociu o lesiu.

CLÀUSULA DE CONFIDENCIALITAT

El present document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació continguda en el mateix és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones, sigui íntegrament o sigui en part, sense el consentiment previ expressat per l'Agència Nacional de Ciberseguretat d'Andorra.