ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Ciberatacs a VPN SSL

TLP: WHITE

FEBRER 2025

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	28/02/2025	03/03/2025

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a 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

Les VPN (Virtual Private Network) SSL (Secure Sockets Layer) són eines fonamentals per garantir la seguretat en la comunicació de les empreses i les organitzacions. Permeten establir connexions segures a xarxes internes a través d'Internet, cosa que esdevé crucial en un entorn cada cop més globalitzat i amb una força remota laboral creixent. Aquestes solucions proporcionen un nivell de confiança elevat en xifrar tot el trànsit entre la xarxa externa i la xarxa interna de l'empresa, per protegir d'aquesta manera la informació delicada contra possibles amenaces.

Tanmateix, a causa del seu ús estès i del paper essencial que exerceixen en la protecció de dades, les VPN SSL també es converteixen en un objectiu atractiu per als ciberdelinqüents. Els atacs a aquestes eines de seguretat són una preocupació creixent en l'àmbit de la ciberseguretat, atès que les VPN SSL són emprades freqüentment per protegir les comunicacions a les xarxes públiques i insegures. L'explotació de vulnerabilitats en aquestes plataformes poden tenir conseqüències greus, des del robatori de dades fins a la interrupció dels serveis crítics de les organitzacions. Per tant, és fonamental adoptar mesures preventives per protegir aquestes connexions.

L'objectiu d'aquest informe és proporcionar una comprensió detallada de les amenaces a les quals s'enfronten les VPN SSL, com també oferir estratègies pràctiques per enfortir-ne la seguretat i minimitzar les possibilitats de ser víctimes d'atacs. En adoptar un enfocament proactiu envers la gestió de riscos i la seguretat de les xarxes internes, les organitzacions podran garantir que les comunicacions continuïn essent segures, fins i tot davant d'un panorama d'amenaces cada vegada més complex i sofisticat.

Al llarg d'aquest informe, s'analitzaran les amenaces i les vulnerabilitats principals associades a les VPN SSL, i es destacaran els mètodes d'atac més comuns que fan servir els ciberdelinqüents. S'abordaran casos específics de vulnerabilitats crítiques que han estat explotades en diverses plataformes de VPN SSL, com també les tàctiques que es fan servir per comprometre la seguretat d'aquestes connexions. A més, es discutiran les millors pràctiques i recomanacions per mitigar aquests riscos, incloses la implementació de mesures de protecció addicional com l'autenticació multifactor, el monitoratge del trànsit i l'actualització contínua del programari de seguretat.

3. DEFINICIONS

Tot seguit, s'estableixen les definicions clau de cara a aquest informe:

3.1. Què són les VPN?

Les VPN (Virtual Private Networks) són xarxes privades virtuals que permeten que els usuaris accedeixin de manera segura a xarxes remotes a través d'Internet. Aquestes proporcionen una capa extra de seguretat atès que xifren el trànsit de dades i emmascaren l'adreça IP de l'usuari. No obstant això, aquesta mateixa capa de protecció les pot convertir en un objectiu per als ciberdelinqüents, que intenten accedir de manera il·legal a xarxes corporatives, robar informació delicada o executar atacs més avançats.

En els darrers anys, l'ús de les VPN ha augmentat considerablement, especialment amb l'auge de la feina remota i l'adopció de models de negoci basats en el núvol.

3.2. Què són les VPN-SSL?

SSL VPN fa referència a una VPN que fa servir un protocol de programari, Secure Sockets Layer. Per a les empreses, aquest tipus de VPN permet que els usuaris remots accedeixin de manera segura a la xarxa corporativa a través d'un navegador web estàndard, sense que calgui instal·lar programari addicional en els dispositius, cosa que simplifica l'accés i millora la flexibilitat.

3.3 Tipus i usos de les VPN SSL

Hi ha dos tipus principals de VPN SSL:

- **VPN SSL de portal**: en aquest tipus de VPN, el terme «portal» es refereix a una porta d'enllaç que proporciona accés als serveis d'una organització mitjançant un lloc web. L'usuari accedeix al portal web de la VPN de l'organització, introdueix les seves credencials i estableix una connexió segura. Una vegada connectat, l'usuari pot accedir a les aplicacions i serveis basats en el web que l'organització ha definit i habilitat.

  Es recomana emprar la VPN SSL de portal quan els usuaris només necessiten accedir a arxius basats en el web, aplicacions i emmagatzematge al núvol. És una opció senzilla i eficient quan les necessitats d'accés es limiten a serveis en línia.

- **VPN SSL de túnel**: en aquesta variant, el terme «túnel» fa referència a un canal segur que es crea entre l'usuari remot i el servidor VPN. Aquest túnel permet que l'usuari no només accedeixi a recursos basats en el web, sinó també a xarxes i aplicacions privades que no són accessibles directament a través d'Internet, sinó que també proporciona un nivell addicional d'accés a sistemes interns de l'organització.

  Aquest tipus de VPN SSL és més adequat per a usuaris que requereixen accés a programari corporatiu, sistemes interns o xarxes privades que no estiguin disponibles públicament a través d'Internet. Aquest model és útil quan cal accedir a una xarxa corporativa completa o a aplicacions que no són accessibles per mitjans tradicionals.

4. PRINCIPALS VULNERABILITATS A LES VPN SSL

Les VPN SSL presenten diverses vulnerabilitats que els atacants poden explotar:

- **Fallades en l'autenticació**: l'ús de credencials dèbils o compromeses com ara contrasenyes simples o repetides, poden permetre que els atacants aconsegueixin accés no autoritzat als recursos protegits per la VPN. A més, si no s'implementen mètodes d'autenticació multifactor (MFA), el sistema pot ser més vulnerable a accessos no desitjats.

- **Explotació de vulnerabilitats del programari**:

  - Fallades en el programari del servidor VPN: per exemple, els atacants poden fer servir les vulnerabilitats zero-day per comprometre la connexió o l'accés a la xarxa interna. Aquestes vulnerabilitats poden ser especialment perilloses si el servidor VPN no es manté actualitzat.
  - Errors de configuració: fa referència a configuracions incorrectes o mal implementades que poden deixar exposats serveis crítics, com ara ports oberts innecessaris, protocols insegurs o permisos mal assignats. Els atacants poden aprofitar aquests erros per penetrar a la xarxa de l'organització o accedir a dades delicades.

- **Atacs a través del trànsit xifrat**: tot i que la connexió VPN està xifrada, els atacants poden intentar explotar mètodes avançats com ara els atacs MitM **(man-in-the-middle)**, en què intercepten i manipulen el trànsit xifrat entre el client i el servidor. Malgrat l'encriptació, si un atacant aconsegueix inserir-se entre tots dos punts, podria obtenir accés a dades confidencials o fins i tot modificar les comunicacions sense ser detectat.

- **Fugues de DNS i filtracions d'IP**: en alguns casos, una configuració incorrecta de la VPN pot provocar fugues de DNS o l'exposició de l'adreça IP real de l'usuari, cosa que podria permetre que els atacants identifiquessin la ubicació i els dispositius de l'usuari. A més, les connexions de xarxes exposades fora del túnels VPN poden ser un punt d'entrada per a ciberatacs.

- **Atacs de denegació de servei (DoS)**: els servidors VPN poden ser objectiu d'atacs DoS o DDoS, cosa que pot interrompre l'accés legítim o sobrecarregar el servidor amb sol·licituds massives, i afectar la disponibilitat del servei i potencialment deixar la xarxa vulnerable a una altra mena d'atac.

5. MÈTODES D'ATAC COMUNS

Entre els mètodes d'atac més comuns hi ha:

5.1 Explotació de vulnerabilitats conegudes

Les vulnerabilitats conegudes són fallades de seguretat en el programari on han estat identificades i documentades i que, sovint, poden ser explotades per atacants si no s'apliquen els pedaços o les actualitzacions corresponents. Aquestes vulnerabilitats poden permetre que els atacants prenguin el control dels sistemes, robin informació o interrompin el funcionament normal de les xarxes i els serveis.

Exemples:

- CVE-2019-19781: una vulnerabilitat crítica a Citrix ADC (que es coneixia anteriorment com NetScaler) va permetre l'execució remota de codi. Els atacants podien enviar sol·licituds al servidor, cosa que els permetia executar comandaments arbitraris en el dispositiu afectat.

- CVE-2020-12812: aquesta vulnerabilitat va afectar la VPN SSL de Fortinet, i va permetre que els atacants eludissin l'autenticació de dos factors. En aprofitar aquesta fallada en el sistema, un atacant podia accedir a les xarxes privades sense que calgués autenticar-se adequadament.

- CVE-2022-26134: una vulnerabilitat en productes d'Atlassian com ara Jira i Confluence, va ser explotada en combinació amb una VPN SSL per executar atacs d'injecció de codi. Els atacants van aprofitar aquesta vulnerabilitat per obtenir accés no autoritzat a les dades delicades emmagatzemades en els sistemes afectats, i van comprometre tant la integritat com la confidencialitat de la informació.

5.2 Força bruta i atac de credencials en massa

Un **atac de força bruta** és l'intent d'inici de sessió en un compte o dispositiu, en el qual s'intenten endevinar les contrasenyes sense context ni pistes. És a dir, es fan servir caràcters a l'atzar que moltes vegades es combinen amb suggeriments de contrasenyes comunes com ara el nom d'usuari i la contrasenya, fins a trobar la combinació correcta. Per altra banda, l'atac de **credencials en massa** és un tipus de ciberatac en el qual les credencials aconseguides per una fuga de dades en un servei es fan servir per intentar iniciar una sessió en un altre servei no relacionat. En tots dos casos, un cop s'aconsegueix l'accés, la presa de control del dispositiu per part dels atacants queda completada, i serveix fins i tot d'accés a la xarxa interna.

Exemple:

La campanya que va començar el 18 de març de 2024 correspon a una sèrie d'atacs de força bruta a gran escala adreçats a serveis VPN i SSH de diversos dispositius de proveïdors com ara Cisco, CheckPoint, Fortinet, SonicWall i Ubiquiti.

Aquests atacs empren una barreja de noms d'usuaris vàlids i genèrics, sense restriccions geogràfiques, cosa que facilita que els atacants accedeixin de manera no autoritzada a les xarxes, bloquejar comptes o provocar interrupcions al servei.

Aquesta activitat no ha tingut un enfocament específic a una indústria, sector o regió en particular, cosa que suggereix una estratègia àmplia d'atac aleatori que cerca una oportunitat de mapar dispositius vulnerables i accessibles que proporcionin l'oportunitat d'un atac específic més perjudicial a les empreses.

Les investigacions van presentar un llistat dels dispositius principals que són objectius:

- Cisco Secure Firewall VPN.
- CheckPoint VPN.
- VPN de Fortinet.
- VPN de SonicWall.
- Miktrotik.
- Draytek.
- Ubiquiti.

5.3 Atacs de programari de segrest

En l'àmbit d'una VPN compromesa, l'atacant pot fer servir la VPN com a una porta d'entrada per infiltrar-se a la xarxa interna de l'organització i desplegar el programari de segrest en múltiples sistemes de xarxa corporativa. Aquest tipus d'atac és particularment perillós perquè les connexions VPN sovint es fan servir per proporcionar accés remot a usuaris dins de la xarxa de l'organització, cosa que pot permetre que els atacants en tinguin accés gairebé il·limitat.

Fer servir la VPN compromesa com a porta d'entrada per desplegar programari de segrest a la xarxa de l'organització podria tenir les conseqüències següents:

- Pèrdua de dades confidencials: accés no autoritzat a informació delicada.
- Disrupció operativa de serveis crítics.
- Impactes financers: costos derivats d'investigacions, multes reguladores, i pèrdua de confiança de clients.
- Compromisos de sistemes crítics: els atacants poden aprofitar les credencials robades per instal·lar programari maliciós o fer moviments laterals dins de la xarxa, i comprometre sistemes addicionals o causar danys més grans.
- Dany a la reputació: les organitzacions poden patir danys a la seva reputació si es filtra informació confidencial o si els clients o usuaris perden confiança en la seguretat de la infraestructura tecnològica.

6. CAS D'ESTUDI: VULNERABILITATS EN PRODUCTES SONIC WALL

A principis del 2025 s'han revelat els detalls d'una vulnerabilitat crítica, la CVE-2024-53704, que permet que els ciberdelinqüents eludeixin l'autenticació en algunes versions de l'aplicació SSL VPN de SonicOS. Això vol dir que els ciberdelinqüents poden segrestar sessions VPN sense que els calguin les credencials i accedir a la teva xarxa com si fossin usuaris legítims.

6.1 CVE-2024-53704

La CVE-2024-53704 (CVSS 8.2) és una vulnerabilitat d'autenticació incorrecta en el mecanisme d'autenticació SSL VPN de SonicOS. Aquest defecte permet que un atacant remot eludeixi l'autenticació i segresti sessions actives de clients SSL VPN. Amb això es dona accés no autoritzat a la xarxa corporativa.

L'explotació de la vulnerabilitat es considera fàcil. L'atac es pot efectuar a través de la xarxa i l'explotació no necessita cap autenticació específica. Se'n desconeixen els detalls tècnics, tot i que se sap que hi ha un explotador disponible.

6.2 Com funciona l'explotador?

Un explotador és una eina o tècnica que es fa servir per aprofitar una vulnerabilitat en un sistema o programari per tal d'executar una acció no autoritzada.

El 22 de gener, investigadors de seguretat van aconseguir desenvolupar un explotador funcional per a aquesta fallada, i van confirmar que era totalment explotable. Després d'oferir als administradors un temps per aplicar els pedaços, finalment es van publicar els detalls tècnics sobre com es du a terme l'atac. En analitzar les respostes del sistema, van confirmar que podien identificar el nom d'usuari, el domini i les rutes privades a les quals tenia accés la víctima a través de la VPN SSL.

L'explotador aprofita una vulnerabilitat en el sistema d'autenticació de l'SSL VPN de SonicWall. L'atac es du a terme amb l'enviament d'una galeta de sessió manipulada, que conté una cadena de bytes nuls codificada en base64, al punt d'autenticació ubicat a '/cgi-bin/sslvpnclient'. Això enganya el sistema, i permet que els atacants accedeixin sense cap mena de restricció.

El problema succeeix perquè el sistema d'autenticació interpreta errròniament la sol·licitud, i assumeix que pertany a una sessió VPN activa. Com a resultat, desconnecta l'usuari legítim, lliura l'accés a l'atacant, i li permet prendre el control total de la sessió.

Un cop dins, l'atacant pot veure els accessos desats a l'oficina virtual de l'usuari, obtenir la configuració del client VPN, establir el seu túnel VPN propi envers la xarxa interna i fins i tot accedir a recursos privats com ara servidors i fitxers compartits.

6.3 Productes afectats i solució

Els productes afectats per la vulnerabilitat crítica CVE-2024-53704 són:

- Tallafocs de la sèrie Gen7, TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700 i NSsp 15700: versions 7.1.x (7.1.1-7058 anteriors), i versió 7.1.2-7019.
- Gen7 NSv, NSv 270, NSv 470 y NSv 870: versions 7.1.x (7.1.1-7058 anteriors), i versió 7.1.2-7019.
- TZ80: versió 8.0.0-8035.
- També hi ha productes afectats per vulnerabilitats de gravetat no crítica.

Com a solució SonicWall recomana actualitzar els productes afectats a les versions de programari:

- Gen6 Hardware Firewalls: 6.5.5.1-6n i superiors.
- Gen7 NSv: 7.0.1-5165 i superiors.
- Gen7 Firewalls: 7.1.3-701 i superiors.
- TZ80: 8.0.0-8037 i superiors.

6.4 Accions que cal prendre

En una publicació del 7 de gener SonicWall va advertir als administradors que han d'actualitzar el seu microprogramari de manera immediata per tancar aquesta bretxa de seguretat. Si es té una SSL VPN o administració SSH habilitada, el tallafocs és vulnerable i s'estaria exposant a un atac real.

- Actualitzar el programari: instal·lar les actualitzacions de seguretat proporcionades per SonicWall per corregir aquesta vulnerabilitat.
- Monitorar la xarxa: vigilar activitats inusuals que poden indicar intents d'explotació.

És essencial que les organitzacions afectades apliquin les actualitzacions de seguretat per protegir les seves xarxes contra possibles atacs.

7. RECOMANACIONS

Una gestió adequada de les configuracions, l'ús de programari actualitzat i la implementació de protocols de seguretat addicionals, com l'autenticació multifactor, són fonamentals per reduir els riscos associats amb les vulnerabilitats identificades.

7.1 Recomanacions generals

Tot seguit es detallen les recomanacions generals:

- **Mantenir el programari actualitzat**: les actualitzacions regulars de programari són crucials, perquè sovint inclouen pedaços de seguretat que corregeixen vulnerabilitats explotables pels atacants. Assegureu-vos d'instal·lar totes les actualitzacions del vostre programari de VPN de manera oportuna per mantenir la xarxa protegida.
- **Habilitar l'autenticació multifactor (MFA)**: l'MFA proporciona una capa extra de protecció en sol·licitar un segon factor d'autenticació, com ara un codi enviat a un telèfon mòbil o generat per una aplicació d'autenticació, a més de la contrasenya. Això fa molt més difícil que els atacants obtinguin accés no autoritzat, fins i tot si aconsegueix desxifrar la contrasenya.
- **Monitoratge i anàlisi del trànsit**: detectar activitats anòmales en temps real.
- **Considerar l'autenticació basada en certificats**: aquesta modalitat proporciona un nivell de seguretat superior en comparació amb l'autenticació tradicional basada només en l'usuari i la contrasenya. Els certificats digitals ofereixen una manera segura de verificar la identitat dels usuaris, i els protegeixen contra atacs de suplantació d'identitat.
- **Capacitar els empleats sobre seguretat cibernètica**: oferir educació continua sobre els riscos de pesca informàtica, enginyeria social i altres tàctiques de ciberatacs. Això garantirà que els empleats estiguin més ben preparats per identificar i evitar amenaces comunes.
- **Auditories de seguretat periòdiques**: revisar configuracions i protocols en ús.
- **Segmentació de la xarxa**: minimitzar els accessos innecessaris i limitar l'abast dels atacs.

7.2 Com protegir les VPN SSL d'atacs de força bruta

Algunes de les millors pràctiques recomanades inclouen:

- **Implementar polítiques de contrasenyes segures**: els usuaris han de tenir contrasenyes complexes i úniques per als seus comptes VPN. Les organitzacions han d'implementar una política de contrasenyes que inclogui requisits de longitud mínima, ús de lletres majúscules i minúscules, nombres, símbols i canvis regulars de contrasenya.
- **Monitorar els intents d'inici de sessió**: és important que es revisin de manera regular els registres de la VPN per identificar comportaments sospitosos com ara múltiples intents fallits d'inici de sessió procedents d'adreces IP no reconegudes. Aquesta pràctica permet detectar i bloquejar possibles atacs de manera avançada.

- **Bloquejar adreces IP sospitoses**: si es detecten adreces IP vinculades a intents de força bruta, és recomanable bloquejar-les per evitar que accedeixin al servidor VPN. Aquesta acció contribueix a prevenir atacs repetits procedents de la mateixa font.
- **Geolocalització VPN**: la majoria de les VPN ofereixen opcions per habilitar la geolocalització. Això permet identificar el país d'origen de cada connexió entrant i bloquejar aquells països que no siguin necessaris.
- **Implementar el filtratge de reputació d'IP**: fer servir serveis de filtratge de reputació d'IP per bloquejar el trànsit procedent d'adreces IP conegudes per la seva activitat maliciosa o sospitosa. Això ajuda a mitigar el risc d'atacs de força bruta i altres amenaces cibernètiques.

8. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté 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 totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.