ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Informe de ciberintel·ligència

Vulnerabilitat crítica MOVEit

TLP:WHITE

21/7/23

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	21/7/2023	21/07/2023

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

Contingut

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. Vulnerabilitat de MOVEit

2.1 CVE-2023-34362

El 27 de maig del 2023 van començar a aparèixer els primers reports d'activitat sospitosa a les xarxes de moltes organitzacions usuàries de MOVEit Transfer. Després de les primeres anàlisis, va confirmar que els actors maliciosos s'estaven aprofitant d'una vulnerabilitat desconeguda per robar dades mitjançant sol·licituds SQL. Aquesta vulnerabilitat es va registrar com a CVE-2023-34362, amb una puntuació de criticitat de 9.8.

El 31 de maig de 2023, Progress Software va anunciar el descobriment d'una vulnerabilitat a MOVEit Transfer. Específicament, es tractava d'una vulnerabilitat d'injecció SQL en l'aplicació web MOVEit Transfer que podria permetre que un atacant no autenticat obtingués accés a la base de dades de MOVEit Transfer.

Segons el motor de la base de dades que s'utilitzi (MySQL, Microsoft SQL Server o Azure SQL), un atacant pot inferir informació sobre l'estructura i el contingut de la base de dades i executar instruccions SQL que alteren o eliminen elements de la base de dades. En el seu anunci, la firma va confirmar que es tractava d'una vulnerabilitat Zero-day i que s'havia estat explotant durant el maig i el juny del 2023.

L'atac a MOVEit Transfer de maig no és el primer del seu tipus. Al gener es van llançar una sèrie d'atacs similars dirigits al GoAnywhere MFT de Fortra i, a finals del 2020, hi va haver una altra explotació massiva d'una vulnerabilitat a Accellion FTA.

Molts atacs tenen com a objectiu l' accés privilegiat als servidors o l' execució de codi arbitrari, la qual cosa també va succeir en aquest cas. No obstant això, sovint l'objectiu dels ciberdelinqüents ha estat l'execució d'un atac ràpid i de baix risc per obtenir accés a les bases de dades d'un servei d'intercanvi d'arxius. Això els ajuda a fer-se amb els arxius sense necessitat de penetrar en el sistema per no romandre massa temps sota el radar. Després de tot, descarregar arxius que estan destinats a ser descarregats no és tan sospitós.

Segons últimes informacions, el nombre d'organitzacions afectades és de 400 i inclou alguns noms realment importants: el Departament d'Energia dels Estats Units i altres agències federals, així com grans corporacions com la companyia d'energia Shell, Deutsche Bank, la firma de consultoria i serveis comercials PwC i el gegant minorista TJX Companies, que va confirmar a The Register el passat 19 de juliol, que "alguns arxius van ser descarregats per un tercer no autoritzat abans que Progress ens notigués la vulnerabilitat"

2.2 Actor d´amenaça Cl0p ransomware

L'atac a MOVEit Transfer va ser reconegut pel grup ransomware Cl0p. A aquest actor d'amenaça se'l coneix també com a FIN11, Clop ransomware group, DEV-0950, UNC902, TEMPWarlock, Lace Tempest i UNC4857. Cl0p ransomware és un cep de ransomware d'alt perfil que ha estat activa des del 2019.

El grup també és conegut popularment per la seva tàctica de "doble extorsió", on les dades robades també amenacen de ser alliberades llevat que es pagui un rescat.

Clop va explotar un desplegament de MOVEit utilitzat pel proveïdor de serveis de nòmina Zellis, els clients del qual inclouen British Airways, la BBC i la cadena de farmàcies Boots a Regne Unit, entre d'altres. Com a resultat, totes aquestes companyies van veure els registres dels seus empleats robats pel grup rus a través de la falla del programari.

Si bé el ransomware generalment es distribueix a través de múltiples tècniques, veiem un augment en el nombre de víctimes a través de vulnerabilitats de programari de servidor. Atès que hi ha múltiples afiliats del grup, a continuació presentem algunes de les tècniques utilitzades:

- Correus electrònics de phishing.
- Explotació de vulnerabilitats.
- Possibilitat de propagar-se a través de credencials exfiltrades de lladres d'informació.
- Vulnerabilitat tipus Zero-day.

3. Com saber si estem afectats?

Si no pots accedir als teus arxius i veus un avís en el teu escriptori que els teus arxius estan encriptats i exigeixen el pagament, és possible que estiguis infectat amb el ransomware Clop.

Clop ransomware va començar a aparèixer en correus electrònics de phishing en algun moment de 2019. Quan xifra arxius, generalment canvia el nom dels arxius agregant una extensió ".clop". Clop utilitza l'estàndard de xifrat RSA i no coneixem cap eina de desxifrat gratuïta i funcional per a Clop.

Així és com pots saber si Clop ransomware ha xifrat les teves dades:

Clop ransomware crearà un arxiu de text anomenat «ClopReadMe.txt» i el col·locarà en cada carpeta xifrada i en el teu escriptori. Si els noms de l'extensió del teu arxiu canvien a ".clop" i veus una nota de rescat que t'indica que pagues als pirates informàtics a través d'un servei web fosc ocult.

Algunes variants de Clop poden eliminar el fons de pantalla del teu escriptori i reemplaçar-lo amb una nota de rescat:

- El teu processador està prop del 100% d'utilització, encara que no estiguis executant cap aplicació de computació intensiva.
- L'ordinador està funcionant més lentament del normal, encara que no estiguis executant cap programa.
- El teu disc dur està llegint i escrivint a gairebé el 100 % de la seva capacitat, encara que no estiguis executant cap aplicació.
- El teu programari antivirus està misteriosament desactivat o no respon.

4. Tecnologia de detecció

Entre les tecnologies utilitzades per a la detecció d'aquesta vulnerabilitat es troba IBM Security QRadar Suite. És una solució modernitzada de detecció i resposta a amenaces dissenyada per unificar l'experiència de l'analista de seguretat i accelerar la seva velocitat al llarg de tot el cicle de vida de l'incident.