TLP:CLEAR
Szabadon terjeszthető!

Tájékoztatás
SonicWall tűzfalakat érintő biztonsági incidensről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki a **SonicWall 7. generációs tűzfalakat** érintő kibertámadás-hullámról, amely során támadók biztonsági réseken keresztül hatoltak be vállalati hálózatokba, többek között ransomware-t is telepítve.

A CVE-2024-40766 azonosítójú, kritikus súlyosságú sérülékenység lehetővé teheti illetéktelen támadók számára a védelmi vonalak megkerülését, hitelesítés kijátszását, valamint az érintett rendszer feletti távoli kódfuttatást.

Az aktív támadások során az **Akira ransomware-t használó támadók** kompromittálták a tűzfalakat, majd rövid időn belül további hálózati elemekre (domain controller) továbbterjeszkedtek, hitelesítési adatokat gyűjtöttek, távoli hozzáféréseket építettek ki, majd ransomware támadást hajtottak végre. A támadások során jellemzően privilegizált fiókokkal (sonicwall, LDAPAdmin) történik a rendszereszközök vezérlése.

A Huntress biztonsági cég szerint **a támadássorozat 2025. július 25-én kezdődött, és azóta is aktívan zajlik**. A támadók a SonicOS kezelőfelületét és az SSLVPN szolgáltatást használták ki, különösen azokon az eszközökön, ahol a 6. generációs beállításokat importálták a 7. generációs eszközökre, és a helyi felhasználói jelszavakat nem változtatták meg. **A SonicWall azóta megerősítette, hogy a támadások ismert, már javított sérülékenységet érintenek, és a hiba elhárítására frissítést is kiadtak.**

Érintettek számára javasolt intézkedések:

- Frissítsék a tűzfal firmware-jét a 7.3.0 verzióra!
- Módosítsák minden helyi SSLVPN hozzáféréssel rendelkező felhasználó jelszavát!
- A SSLVPN szolgáltatás ideiglenes kikapcsolását, ha az nem szükséges.
- Ha a szolgáltatás nem kapcsolható ki, korlátozzák az elérhetőséget ismert, megbízható IP-címekre!
- Vizsgálják felül a szolgáltatói fiókok jogosultságait, különösen a „sonicwall” és „LDAPAdmin” típusúakat! Ezek ne rendelkezzenek Domain Admin jogosultságokkal!
- Többfaktoros hitelesítés kötelező alkalmazása minden távoli elérés esetén, azonban ez nem garantál teljes biztonságot.
- **Botnet védelem és Geo-IP szűrés aktiválása** az SSLVPN kapcsolatnál.
- Nem használt felhasználói fiókok eltávolítása.
- Jelszavak rendszeres frissítése minden felhasználói fiókban.

Támadási módszerek rövid összefoglalása:

A támadók először adminisztratív hozzáférést szereztek. Ezt követően Cloudflared és OpenSSH segítségével backdoort telepítettek. Az eszközökön belül WMI és PowerShell segítségével oldották meg az oldalirányú mozgást, és hitelesítő adatokat gyűjtöttek, többek között a Veeam Backup és az Active Directory adatbázisokból. Biztonsági megoldásokat kapcsoltak ki, köztük a Microsoft Defender-t és a Windows tűzfalat.

A támadások vége jellemzően Akira zsarolóvírus telepítése volt, árnyékmásolatok törlésével együtt.

Mitigáció:

- Az SSL VPN szolgáltatás letiltása a SonicWall eszközön.
- A VPN hozzáférés korlátozása IP-szűréssel.
- A rendszer átvizsgálása ismert támadási jelek (IoC-k) alapján.

Kapcsolódó IoC-k:

42.252.99[.]59	Támadó IP
45.86.208[.]240	Támadó IP
77.247.126[.]239	Támadó IP
104.238.205[.]105	Támadó IP
104.238.220[.]216	Támadó IP
181.215.182[.]64	Támadó IP
193.163.194[.]7	Támadó IP
193.239.236[.]149	Támadó IP
194.33.45[.]155	Támadó IP
w.exe, win.exe sha256: d080f553c9b1276317441894ec6861573fa64fb1fae46165a55302e782b1614d	Ransomware végrehajtható fájl
C:\ProgramData\winrar.exe	Adat előkészítő eszköz
C:\ProgramData\OpenSSHa.msi	OpenSSH installer
C:\Program Files\OpenSSH\sshd.exe	SSH fájl exfilhez
C:\programdata\ssh\cloudflared.exe	Cloudflare fájl
C:\Program Files\FileZilla FTP Client\fzsftp.exe	Adat szivárogtató eszköz
C:\ProgramData\1.bat	Támadó script
C:\ProgramData\2.bat	Támadó script
AS24863 - LINK-NET - 45.242.96.0/22	ASN/CIDR ellenséges infrastruktúra

AS62240 - Clouvider - 45.86.208.0/22	ASN/CIDR ellenséges infrastruktúra
AS62240 - Clouvider - 77.247.126.0/24	ASN/CIDR ellenséges infrastruktúra
AS23470 - ReliableSite LLC - 104.238.204.0/22	ASN/CIDR ellenséges infrastruktúra
AS23470 - ReliableSite LLC - 104.238.220.0/22	ASN/CIDR ellenséges infrastruktúra
AS174 - COGENT-174 - 181.215.182.0/24	ASN/CIDR ellenséges infrastruktúra
AS62240 - Clouvider - 193.163.194.0/24	ASN/CIDR ellenséges infrastruktúra
AS62240 - Clouvider - 193.239.236.0/23	ASN/CIDR ellenséges infrastruktúra
AS62240 - Clouvider - 194.33.45.0/24	ASN/CIDR ellenséges infrastruktúra
backupSQL	A támadó által létrehozott felhasználó
lockadmin	A támadó által létrehozott felhasználó
Password123$	A támadó által használt jelszó
Msnc?42da	A támadó által használt jelszó
VRT83g$%ce	A támadó által használt jelszó

TLP:CLEAR
Szabadon terjeszthető!

A gyártói biztonsági közlemény itt érhető el:

https://www.sonicwall.com/support/notices/gen-7-sonicwall-firewalls-sslvpn-recent-threat-activity/250804095336430

További információ:

https://cert.europa.eu/publications/security-advisories/2025-029/

https://www.huntress.com/blog/exploitation-of-sonicwall-vpn

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833