CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-046

Zerologon Critical Vulnerability Affecting Windows Domain Controllers

September 25, 2020 — v1.1

TLP:WHITE

History:

- *15/09/2020 — v1.0 – Initial publication*
- *25/09/2020 — v1.1 – Updated with details on attacks, SAMBA, and new detection methods*

Summary

On 11th of August 2020, Microsoft released a critical security advisory affecting all supported versions of Windows Server [1]. The vulnerability is described as *Netlogon Elevation of Privilege* and got assigned CVE-2020-1472 [2].

On 11th of September 2020, Secura released a white paper [3] and testing tool [4] for the vulnerability. The paper[1] describes how an attacker with a foothold on a victim network could leverage this vulnerability to compromise an unpatched Domain Controller. The attacker can obtain domain admin privileges by taking advantage of flaws in a cryptographic authentication protocol.

Starting on the 14th of September 2020, several *security researchers* modified the initial testing tool created by Secura to provide full proof of concept of the vulnerability, allowing any attacker with a foothold on a victim network to easily elevate its privileges to domain admin.

On 23rd of September 2020, SAMBA also released security patches addressing the vulnerability, explaining that SAMBA server is vulnerable if used as a Domain Controller [10].

On 24th of September 2020, Microsoft Security Intelligence warned that ongoing attacks were being observed abusing Zerologon vulnerability [6].

[1] *Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472)*

Technical Details

The vulnerability was assigned *CVE-2020-1472* [2] with a CVSS score of 10.

The core of the vulnerability is due to an insecure use of AES-CFB8: When using EAS, the `ComputeNetlogonCredential` function makes use of CFB8 (8-bit cipher feedback) mode for block cipher operation, but wrongly uses a fixed value as an initialisation vector (16 zero bytes). Because of that, for 1 in 256 keys, applying AES-CFB8 encryption to an all-zero plaintext will result in all-zero ciphertext.

Several steps are then needed to exploit this weakness:

- Step 1: Spoofing client credentials by using brute-force authentication attack (average attempts: 256) with a challenge value of 8 zeroes.
- Step 2: Disabling signing and sealing by unsetting a flag in the `NetrServerAuthenticate3` call, leading to requesting a session without encryption.
- Step 3: Spoofing the first call after authentication by setting timestamp value to 0 (January 1st, 1970).
- Step 4: Changing a computer's AD password by using the `NetrServerPasswordSet2` call with a plaintext value of 516 zeroes, which lead to the computer password to be set as empty.
- Step 5: From password change to domain admin by performing the attack on the Domain Controller itself and running a DCsynch attack with the newly emptied password.

Detection

Since the initial release of information about this vulnerability, several security researchers provided more information on detection of Zerologon attacks [7, 8]. Also Microsoft provided a way to enforce usage of secure RPC with Netlogon secure channel between member computers and Active Directory (AD) Domain Controllers (DC) [9].

There is three specific steps of the attack which provide possibilities for defenders to detect exploitation of the vulnerability:

Initial Spoofing of Client Credentials

When initiating the attack, it is necessary to perform several authentication attempts before getting the expected cyphertext value (all-zero) as described in the tester script [4]:

```
# Keep authenticating until successful. Expected average number of attempts needed: 256.
```

It means that several events may be triggered during this step of the attack so some monitoring may be used to detect attempts to exploit the vulnerability:

- Monitor network traffic for high number of `NetrServerReqChallenge` and/or `NetrServerAuthenticate3` RPC operations
- Monitor Windows events for high number of failed machine account netlogon authentication on domain controller (EventID=5805)

DCSync

The last step of the attack consist of performing a DCSync attack on the targeted Domain Controller (In the paper, researcher use *Impacket's* `secretsdump` script). It means that usual way to detect DCSync attack can be used:

- Monitor network traffic for `DRSUAPI` RPC requests (operation `DsGetNCChanges`) and compare the source host against a list of known domain controllers
- Monitor Windows events for EventID 4662 with GUID = `{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}` (`DS-Replication-Get-Changes-All` Control access right) [5]

Modification of machine credentials

When the attack is successful, computer's AD password will be modified, triggering one or several detection possibilities:

- Monitor Windows events for Change of computer account (EventID=4742) by an anonymous logon
- Monitor Windows events for succesful login (EventID=4624) followed by an password account reset (EventID=4624)

Products Affected

This vulnerability affects the following Microsoft Server versions:

- 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)

This vulnerability also affects SAMBA server if used as Domain Controller:

- Samba 4.0 and later

Recommendations

CERT-EU recommends updating following Microsoft guidance as soon as possible [1].

If some 3rd party devices needs to communicate with Domain controllers, it is also recommended to enforce usage of secure RPC with Netlogon secure channel and create exceptions for devices not able to communicate securely, as described by Microsoft [9].

Regarding SAMBA server, if used as domain controller, it is also highly recommended to patch as soon as possible [10].

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472

[3] https://www.secura.com/pathtoimg.php?id=2055

[4] https://github.com/SecuraBV/CVE-2020-1472/blob/master/zerologon_tester.py

[5] https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/1522b774-6464-41a3-87a5-1e5633c3fbbb

[6] https://twitter.com/MsftSecIntel/status/1308941504707063808

[7] https://www.lares.com/blog/from-lares-labs-defensive-guidance-for-zerologon-cve-2020-1472/

[8] https://blog.zsec.uk/zerologon-attacking-defending/

[9] https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

[10] https://www.samba.org/samba/security/CVE-2020-1472.html