National Cyber Security Centre
a part of GCHQ

Alert: UK organisations should patch Netlogon vulnerability (Zerologon) after actor exploitation

Version 1.0

25 September 2020

Introduction

In late September 2020, Microsoft confirmed that actors were actively exploiting the escalation of privilege vulnerability affecting Microsoft Windows Netlogon, or CVE-2020-1472. This exploit is also referred to as Zerologon.

This vulnerability has been widely documented online and it is reported that publicly available tools such as Mimikatz and Metasploit have been updated to include an exploit for this vulnerability.[1]

In August Microsoft made available security updates to mitigate malicious activity, the details of which are included in this alert. Microsoft is tracking threat actor activity and monitoring developments.[2]

Details

A vulnerability in the Netlogon Remote Protocol allows an attacker with network access to a Domain Controller to impersonate any domain user and change their account password. This includes the ability to change the Domain Admin account password, leading to compromise of the Domain Controller. The attacker does not need to be domain joined.

Affected products

Any version of Windows Server with the Domain Controller role installed, not patched with the 11/08/2020 update, is vulnerable. This includes the following versions:

Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Windows Server version 1903
Windows Server version 1909
Windows Server version 2004

Mitigation

Mitigating this vulnerability is a two stage process:

1. Ensure that all Domain Controllers have the August 2020 security update applied.

[1] https://twitter.com/gentilkiwi and https://github.com/rapid7/metasploit-framework/pull/14151

[2] https://twitter.com/MsftSecIntel/status/1308941504707063808?ref_src=twsrc%5Etfw

2. Enable Domain Controllers (DC) enforcement mode − either via a registry key or by applying the 9 February 2021 security update when it is available.

Domain Controller enforcement mode

After installing the August 2020 security updates, Domain Controller (DC) enforcement mode can be enabled through a registry key ahead of the 9 February 2021 security update.

DC enforcement mode is when all Netlogon connections are either required to use secure RPC or when the account has been added to the 'Domain controller: Allow vulnerable Netlogon secure channel connections' group policy.

Links and guidance

For information from Microsoft on both the August 2020 and February 2021 updates for CVE-2020-1472, visit:

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

More information on CVE-2020-1472 specifically is available at:

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

Other methods of exploitation

New evasion and exploitation techniques for this vulnerability beyond the password reset have recently emerged and oy hers are likely to follow.[3] Threat hunts for this technique will need to take account of these developments and make use of new detection strategies as they emerge.

Detection

Artifacts

When an actor exploits this vulnerability, it may leave behind various artifacts which can be used for detection. The most documented artifact is Windows Event ID 4742 'A computer account was changed', often combined with Windows Event ID 4672 'Special privileges assigned to new logon'.

Detecting vulnerable hosts

This script will recursively query all the domain controllers within the Forest, using WMI to retrieve the Domain Controller Name, Operating System (OS) and installed KB:

[3] For example, the 'printer bug' using the NTLM protocol detailed here: https://dirkjanm.io/a-different-way-of-abusing-zerologon/ and use of DCSync https://www.lares.com/blog/from-lares-labs-defensive-guidance-for-zerologon-cve-2020-1472/

https://github.com/cisagov/cyber.dhs.gov/tree/master/assets/report/ed-20-04_script

Signatures

CVE-2020-1472 (CISA ED 20-04) can be detected using Splunk Attack Range:

https://www.splunk.com/en_us/blog/security/detecting-cve-2020-1472-using-splunk-attack-range.html

A YARA rule is available:

https://go.cynet.com/hubfs/rule%20Zerologon.yara

A SNORT rule for possible Mimikatz exploitation of CVE-2020-1472 is available:
https://gist.github.com/silence-is-best/435ddb388f872b1a2e332b6239e9150b

Sigma rules are available:
https://blog.zsec.uk/zerologon-attacking-defending/#detection-response-monitoring-for-attacks

Conclusion

The NCSC **strongly advises** that organisations refer to the Microsoft guidance referenced in this alert and ensure the necessary updates are installed in affected Netlogon products.

The NCSC generally recommends following vendor best practice advice in the mitigation of vulnerabilities. In the case of the Zerologon exploit, the most important aspect is to install the latest patches as soon as practicable.