"Zerologon" Netlogon Remote Protocol Vulnerability

Executive Summary

In August, Microsoft released a patch for a vulnerability that is applicable to the healthcare community. CVE-2020-1472, also called Zerologon, was rated critical severity as it allows unauthenticated administrative access to a Windows domain controller (DC) and possible compromise of the entire domain. Applying the Microsoft patch will completely resolve this vulnerability, which HC3 recommends patching of vulnerable systems be prioritized for any healthcare organization.

Analysis

A domain controller is critical to any network as it validates and authenticates users of various levels of authority to determine who gains access to network resources. Exploitation of a domain controller allows an attacker to compromise the entire network and all resources it contains and therefore should be considered a high priority. Microsoft Windows domain controllers contain a flaw in a cryptographic authentication scheme (AES-CFB8) used by the Netlogon Remote Protocol allowing an attacker with only user-level access to gain administrative access. This would provide the attacker with additional opportunities including the creation of accounts for persistence as well as the compromise data on the network and the disruption of functionality of connected systems potentially impacting patient care.

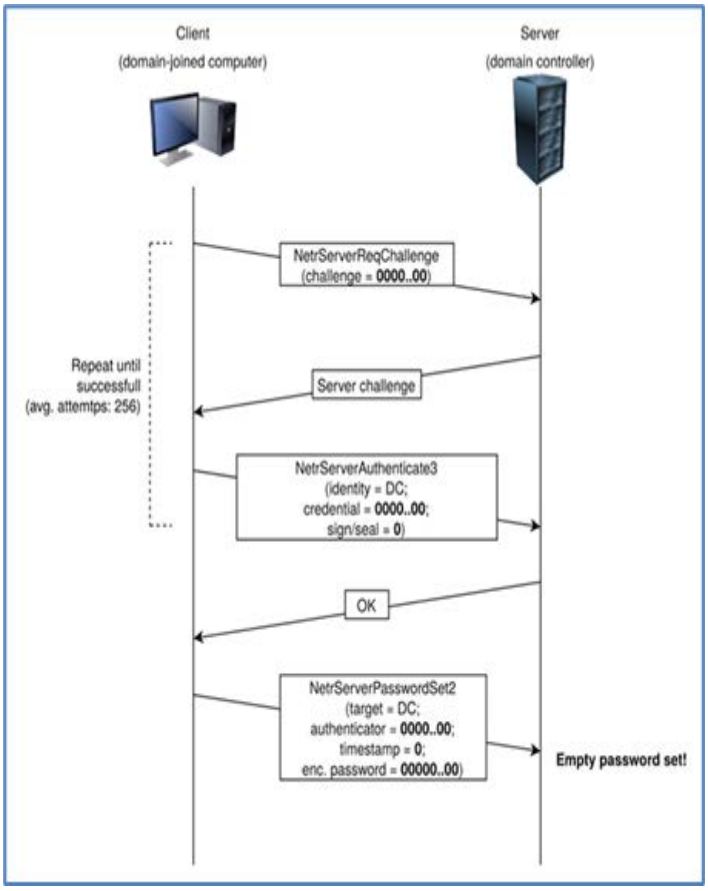

Figure 1 EXAMPLE OF ZEROLOGIN ATTACK Credit: Secura

Alert

Microsoft released first phase update CVE-2020-1472 on August 11, 2020, with the second phase planned for February 9, 2021. The first phase enforces secure Remote ProtoCol (RPC) usage for machine accounts on Windows based devices, trust accounts and all Windows and non-Windows DCs. Within the new update, a new group policy is available as well as a secure registry key. CVE-2020-1472 affects supported Windows Server versions listed below:

- 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)

Patches, Mitigations & Workarounds:

HC3 recommends identifying all vulnerable enterprise systems and taking the following mitigation actions on each system in question:

- Install the update on all DCs and read-only domain controllers (RODCs Operationalization of Indicators of Compromise) CVE-2020-1472
- Address non-compliant devices that are using vulnerable Netlogon secure channel connections. After updates are applied to DCs, events can be collected in DC event logs to determine which devices in your environment are using vulnerable Netlogon connections.
- Monitor for warning events and assess. Use available event monitoring software or scripts to monitor DCs.

References

CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

[MS-NRPC]: Netlogon Remote Protocol
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nrpc/ff8f970f-3e37-40f7-bd4b-af7336e4792f

How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472
https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc
Exploit for Netlogon Remote Protocol Vulnerability, CVE-2020-1472
https://us-cert.cisa.gov/ncas/current-activity/2020/09/14/exploit-netlogon-remote-protocol-vulnerability-cve-2020-1472?s=03

Are your domain controllers safe from Zerologon attacks?
https://www.helpnetsecurity.com/2020/09/15/cve-2020-1472/

After researchers test Microsoft Netlogon exploit, feds tell users to patch now or suffer later
https://www.cyberscoop.com/microsoft-netlogon-exploit-secura/

Exploit code for 'Zerologon' bug impacting Windows Netlogon Remote Protocol published on Github
https://www.computing.co.uk/news/4020182/exploit-code-zerologon-bug-impacting-windows-netlogon-remote-protocol-published-github

New Windows exploit lets you instantly become admin. Have you patched?
https://arstechnica.com/information-technology/2020/09/new-windows-exploit-lets-you-instantly-become-admin-have-you-patched/