Serianu Cyber Security Advisory

CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability

Serianu SOC Advisory Number:

TA – 2020/015

Date(s) issued:

13th October, 2020

Systems Affected

- Domain Controller

OVERVIEW:

The Serianu research team is sharing this technical alert to advice IT professionals and managers in organizations, to increase priority on patching vulnerabilities that are increasing being exploited by sophisticated malicious actors. This alert explains the full impact, execution and recommendation of the vulnerability, identified as CVE-2020-1472.

Analysis

CVE-2020-1472 also known as Zerologon, is a critical vulnerability affecting all versions of supported Microsoft Windows Server (Windows 2008 R2, 2012, 2016, 2019). An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC).

Netlogon is a Windows Server process that authenticates users and other services within a domain. The Netlogon Remote Protocol is used to change or replicate account credentials and passwords within a domain, as well as maintain user domain controller (DC) relationships. A domain controller is a server that responds to security authentication requests in a Windows environment. A compromised domain controller can give attackers access to a corporate network.

To exploit this vulnerability, an attacker would need to launch the attack from a machine on the same Local Area Network as their target server.

The vulnerability allows an attacker to forge an authentication token for Netlogon and remove or change the password of any computer account on the domain controller. Thereafter an attacker can use the new password to take over the domain controller, alter credentials, escalate privileges or move laterally within the domain. Further exploits show the ability of this being used to deploy malware, dump credentials and hashes.

Detection:

The attack can be challenging to detect as the attacker is authenticating to the domain in a manner resembling legitimate account behavior and the exploit leaves very few traces in the event logs besides a password reset.

Recommendation:

1. Microsoft rolled out a phased approach to remedy this vulnerability. Phase 1 has seen them release a patch for CVE-2020-1472 (Zerologon) in August's Patch Tuesday 2020.
2. Organizations that have not already updated affected systems should patch immediately and review any indicators of compromise (IOC).
3. All supported servers should be patched as soon as possible. The second phase is expected in Q1 of 2021.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to commonly exploited vulnerabilities to share it with us through our email info@serianu.com to allow us to analyse any indicators of compromise (IOC).