ultraviolet

CONFIDENTIAL

THREAT REPORT:

ZeroLogon: Something for Nothing

Services Performed By:
UltraViolet Cyber
Meredith Glass
(443) 351-7630
info@uvcyber.com

Published Date:
April 4, 2024

Contents

1 Executive Summary

ZeroLogon is a Windows Netlogon vulnerability first detected in 2020. CVE-2020-1472 was assigned for this vulnerability. [5] While Microsoft has released appropriate patching for this vulnerability following its discovery with several updates since, it is important for companies to recognize that this vulnerability is still actively being searched for and exploited to gain unmitigated access to domain controllers and thereby entire networks. Please read on for more details on this vulnerability, its functionality and what steps can be taken to protect vital systems from threat actors employing this attack vector.

2 Technical Analysis

ZeroLogon leverages a weak cryptographic algorithm (AES-CFB8) that the Netlogon authentication process utilizes. Attack is done using 0 characters in Netlogon authentication parameters. Allows for password changes across all of AD, attacker gains access to disabling security features and allows for impersonation of any device in network/AD. [2]

Exploit Process:

1) Brute-force attack domain controller with 8 zero-byte challenge/cyphertext spoofing the identity of DC to establish unsecure Netlogon channel. It has been noted that the average number of attempts is around 256 with a probability of 1:256 success. In reviewing PoC code for scripts published to enumerate and/or exploit this vulnerability, usually max tries are somewhere around 2000.
2) NetrServerPasswordSet2 call is used to set DC account password to empty value in AD. This is destructive toward DC functionality and requires an additional step listed below.
3) Domain Replication Service (DRS) Protocol is utilized with empty password to connect to same DC and dump hashes.
4) It is necessary to revert DC password to the original stored in local registry to prevent detection.
5) Hashes dumped from step 3 can be used to perform a variety of attacks (PTH, Golden Ticket, etc.)

Notably, ZeroLogon can be pulled into the Mimikatz toolkit, also. [1]

Impacket is used alongside ZeroLogon exploitation to pull hashes from the DC. Full domain takeover is possible utilizing this type of attack.

The ZeroLogon attack does need to come from a machine on the same LAN as the target and the spoofed login must function in the same fashion as a domain login attempt. Because AD must 'see' (recognize) the client attempting connection within the communication mechanism architecture (logical topology), external addresses would be extremely unlikely to have any success in exploiting this vulnerability. Hence, this vulnerability and exploitation thereof falls under the category of 'Privilege Escalation', for the most part. [2]

Microsoft revealed use of the ZeroLogon attack to access government systems with persistence attributed to Mercury APT group. [3] The Trickbot trojan has also been seen utilizing ZeroLogon to achieve objectives. [4]

In an article from the Healthcare IT Journal by Murphy Miller, some additional useful information pertaining to campaigns utilizing ZeroLogon and related activity preceding exploitation of the Netlogon vulnerability was presented, as follows:

CISA and the FBI revealed in the notification that attacks commence with the exploitation of legacy vulnerabilities located in VPNs and network access devices. In many attacks, preliminary access to networks was obtained via exploitation of vulnerability CVE-2018-13379 of the Fortinet FortiOS Secure Socket Layer (SSL) VPN as well as the MobileIron vulnerability CVE-2020-15505. Ransomware gangs are likewise taking advantage of the last-mentioned vulnerability subsequent to the advisory of a PoC exploit for the flaw.

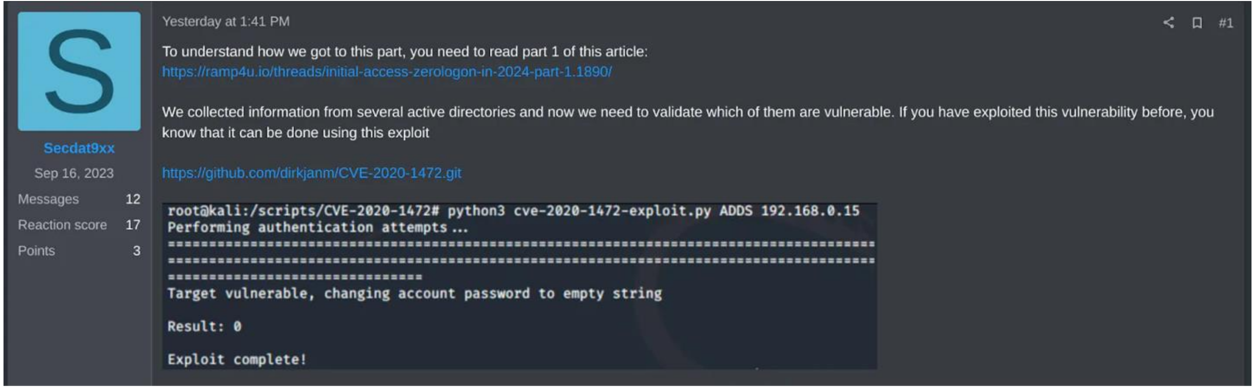
Although the most current campaigns were performed exploiting the previously mentioned vulnerabilities, CISA/FBI advises that there are some other legacy vulnerabilities in Internet-facing infrastructure that may, in the same way, be taken advantage of in attacks for example:

- *CVE-2019-19781 – Citrix Gateway/Citrix SD WAN WANOP vulnerability*
- *CVE-2020-5902 – F5 BIG-IP vulnerability*
- *CVE-2019-11510 – Pulse Secure vulnerability*
- *CVE2019-19751 – Citrix NetScaler vulnerability*
- *CVE-2020-2021 – Palo Alto Networks vulnerability*
- *CVE-2020-1631 – Juniper vulnerability*

Very recently, in an article published by ZeroFox, intel from threat actor Secdat9xx posted on the RAMP community site a sort of manual indicating that ZeroLogon is very much still being exploited 'in the wild' and essentially gave a how to guide in the manual:

> *ZeroLogon is a privilege-elevation vulnerability with a NIST severity score of 10.0 (critical). Successfully exploited, it enables threat actors to establish a vulnerable Netlogon secure channel connection to a domain controller using the Netlogon Remote Protocol (MS-NRPC). This can enable the attacker to gain domain administrator access.* [6]

*Also including image shared by ZeroFox Intelligence showing the Secdat9xx post: ￼



Secdat9xx
Sep 16, 2023
Messages 12
Reaction score 17
Points 3

Yesterday at 1:41 PM

To understand how we got to this part, you need to read part 1 of this article:
https://ramp4u.io/threads/initial-access-zerologon-in-2024-part-1.1890/

We collected information from several active directories and now we need to validate which of them are vulnerable. If you have exploited this vulnerability before, you know that it can be done using this exploit

https://github.com/dirkjanm/CVE-2020-1472.git

```
root@kali:/scripts/CVE-2020-1472# python3 cve-2020-1472-exploit.py ADDS 192.168.0.15
Performing authentication attempts ...
======================================================================================
======================================================================================
===============================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

The ease at which threat actors can acquire the necessary tools to make use of and exploit this vulnerability is staggering; all that is required is the ZeroLogon PoC, CrackMapExec (both on GitHub publicly) and employ a Metasploit module to remove an administrator password. [6]

Microsoft suggests rejecting NetrServerAuthenticate3 requests with the first five bytes being identical as well as rejecting unsigned/unsealed Netlogon channels on all Windows accounts. At this time, Microsoft should have further increased the scope of the patching that occurred to include rejection of insecure Netlogon sessions from non-Windows devices. MS fixed the vulnerability by enforcing RPC (remote procedure call) in Netlogon Protocol across all Windows devices. [1] [2]

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber is actively threat hunting for IoCs and artifacts related to emerging threats
- Monitoring authentication activity to ensure no suspicious or malicious behavior is occurring
- Communicating with customers promptly when vulnerabilities that may be exploited are shown to be present either via threat hunting or in information gathered during normal workflow

4 What Customers Can Do

- Ensure patching is up to date on all devices where this is feasible
- Maintain proper segmentation or isolation for legacy devices to ensure access is limited to authorized users from authorized hosts within organization
- Utilize GPO to require DC (domain controllers) to use secure Netlogon with the exception of devices that support only the insecure Netlogon version.

5 References

[1] https://www.crowdstrike.com/blog/cve-2020-1472-zerologon-security-advisory/
[2] https://www.tenable.com/blog/cve-2020-1472-zerologon-vulnerability-in-netlogon-could-allow-attackers-to-hijack-windows
[3] https://www.healthcareit.tech/cisa-fbi-advisory-on-apt-groups-chaining-legacy-vulnerabilities-along-with-netlogon-vulnerability/
[4] https://www.malwarebytes.com/blog/news/2021/01/the-story-of-zerologon
[5] https://nvd.nist.gov/vuln/detail/CVE-2020-1472
[6] https://www.zerofox.com/blog/the-underground-economist-volume-4-issue-6/
[7] https://woshub.com/zerologon-critical-active-directory-vulnerability/