<)FORESCOUT.

Zerologon Vulnerability

FAQ: Identify & Mitigate Risk with Forescout

Q: What is Zerologon?

A: Zerologon is an elevation of privilege vulnerability that allows an attacker to gain access to Windows Domain Controllers by utilizing a vulnerable Netlogon secure channel connection via Netlogon Remote Protocol (MS-NRPC). The name "Zerologon" is derived by the exploit's use of zero characters in Netlogon authentication parameters during the session initiation between the client and the server. This vulnerability received a CVSS score of 10/10. It can be carried out in seconds with little experience and can change passwords on domain controllers. One caveat: the attacker must have an initial foothold in the network to execute the attack.

Q: Is my organization vulnerable?

A: It is highly likely that organizations could have vulnerable domain controllers, depending on patching schedules. The Zerologon vulnerability impacts: Windows Server 2008 R2 SP1 64-bit, Windows Server 2012 (all versions), Windows Server 2016 (all versions), Windows Server 2019 (all versions), and Windows Server 1903, 1909, 2004 (Server Core Installations.) Microsoft is rolling out patches in a two-phased approach. More on patches below.

Q: How does it impact devices?

A: If an attacker has a foothold on the network via a compromised system or is able to gain physical access to the network, they can reset the domain controller password in seconds and take over the entire domain. Furthermore, failure to follow proper deployment guidelines during the patching process could cause outages for domain controllers or other non-Windows systems that rely on MS-RPC.

Q: Can Forescout help identify vulnerable devices?

A: Yes. Forescout has released a Security Policy Template (SPT) for eyeSight, which helps organizations automate the detection of vulnerable devices. The SPT automatically identifies Windows servers on the network and attempts a Netlogon negotiation using the zeroed authentication parameters. If successful, Forescout closes the connection preventing payload delivery and flags the affected systems as vulnerable devices.

If the servers are managed by Forescout eyeSight, either agentlessly or via SecureConnector™, a policy could also be written to check for the presence of the FullSecureChannelProtection registry key that was introduced in the August 11, 2020 patch. Also, if the FullSecureChannelProtection registry key is set to '0', domain controllers will still allow vulnerable Netlogon secure channel connections from non-Windows devices.

Q: Can I patch vulnerable devices?

A: Yes. Microsoft released the first patch on August 11, 2020, in KB4565351, which protects Windows devices from the exploit. It also adds event IDs in System event logs for monitoring when connections are denied, allowed by a Group Policy Object (GPO), or allowed via a vulnerable connection. Depending on how the patch was implemented, non-Windows devices could still be permitted to connect to domain controllers using the vulnerable AES-CFB8 cipher.

The second patch is expected February 9, 2021. This patch will enforce the proper Netlogon secure channel connections for both Windows and non-Windows devices unless noncompliant devices are explicitly allowed via a GPO. As mentioned above, if the proper Microsoft guidelines aren't followed, this patch could cause outages.

Q: How else do I mitigate risks from Zerologon?

A: Following a proper defense-in-depth strategy is always advised.

- As mentioned above, Forescout eyeSight can be used with the new Zerologon SPT policy to identify vulnerable networked servers automatically. If devices are manageable, the system can also check for the presence of patches and the protection registry key.

- Since the attacker requires an existing foothold on the network with access to the domain controller, eyeSight can help ensure proper compliance of managed endpoints on the network. eyeSight achieves this by validating that all endpoint protection agents are installed, running and updated properly.
- For non-manageable endpoints, Forescout eyeSight, eyeControl and eyeSegment can restrict access from IoT devices or unmanaged systems that don't require direct access to the domain controllers. These devices often can't be patched and can't run endpoint protection agents, so limiting their access can drastically reduce their use as an attack vector.

Q: I am a Forescout eyeInspect (formerly SilentDefense™) customer. Can I detect Zerologon events on my network?

A: Yes. Forescout created a SilentDefense script for customers. The script monitors network communications to detect a system that attempts the exploit. It watches for two specific messages on the network while a Netlogon session is being negotiated. The first is a NetrServerReqChallenge message containing eight bytes of zero. The second is a NetrServerPasswordSet2 message that is used to overwrite the domain controller password with 512 bytes of zero. If either message is detected, an alert can be triggered. This information can also be coupled with Forescout eyeSight and eyeControl to take an immediate, automated response.

Additional Resources:

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

Secura whitepaper documenting the findings: https://www.secura.com/pathtoimg.php?id=2055

Secura script to identify vulnerable DCs: https://github.com/SecuraBV/CVE-2020-1472

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

More information on patches, event IDs, and patch deployment guidelines: https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc