SecurityRisk ADVISORS

CyberSOC Threat Notification

Microsoft Netlogon Privilege Escalation Vulnerability

Executive Summary

On August 11th, 2020 Microsoft released a security update detailing a vulnerability dubbed "Zerologon" affecting the Netlogon Remote Protocol (MS-NRPC). A flaw exists in the encryption scheme of the Netlogon authentication process which an attacker can abuse to gain domain administrator access.

Description

An unauthenticated attacker can exploit this vulnerability by using the Netlogon protocol to connect to a domain controller. Successful exploitation of this flaw could allow an attacker to impersonate machines, disable security features, and update computer passwords. Proof of concept (PoC) code has been published on GitHub.

Affected Products

- Windows Server 2008 R2
- Windows Server 2012 & Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)
- Windows Server, version 2004 (Server Core installation)

Safeguards/Recommendations

Microsoft is addressing the vulnerability in a two-part rollout. The first patch was released in the August Patch Tuesday updates and the second phase of updates will become available in Q1 2021. Affected customers are strongly encouraged to apply the patch.

Update: The Netlogon vulnerability is actively being exploited in the wild. Organizations should create an inventory of all vulnerable devices which should be monitored and patched in the second phase of updates. A workaround currently exists which involves setting a group policy and adding a new registry key.

Vendor: Microsoft

CVE-ID: CVE-2020-1472

Published: Aug 11, 2020

CVSS V3 Overall score: 10

Criticality: Critical

Patch Availability: Patch Available

Vulnerability Type: Privilege Escalation

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Changed

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Proof of Concept

Remediation Level: Official Fix

Report Confidence: Confirmed

Devices should be monitored for event IDs 4742, 5805, 4624, and 4662 with indicators of Zerologon activity. Patched domain controllers should also be monitored for events with event ID 5829. Detection logic has been released to detect events related to the Netlogon exploit using Snort and Zeek/Bro. Other detection methods were published including a Yara rule which detects Zerologon in memory dumps of lsass.exe and a Sigma rule which detects activity based on event IDs.

References

- https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc
- https://us-cert.cisa.gov/ncas/current-activity/2020/09/14/exploit-netlogon-remote-protocol-vulnerability-cve-2020-1472
- https://www.sentinelone.com/blog/zerologon-cve-2020-1472-sentinelone-first-to-detect-on-the-endpoint/
- https://blog.zsec.uk/zerologon-attacking-defending/
- https://www.lares.com/blog/from-lares-labs-defensive-guidance-for-zerologon-cve-2020-1472/
- https://blog.talosintelligence.com/2020/09/netlogon-rises.html
- https://gist.github.com/silence-is-best/25ae0929c277642e86ecf592598a3254
- https://github.com/corelight/zerologon

Version History

Version 2. Report Update

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io