|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Group 1955695160, Grouped object |  | Machines Vulnerable to Zerologon (CVE-2020-1472) | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | Critical | **CVSS v4.0 Score** | 9.3 |
| **CVSS Vector** | | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N | | |

Technical Description

The Zerologon (CVE-2020-1472) vulnerability is a critical vulnerability in the cryptographic authentication scheme used by the Netlogon Remote Protocol, which can be used for different tasks including updating computer passwords.

Any unauthenticated attacker with server access can send specially crafted packets and change the machine account password. An attacker can then authenticate to the domain with the compromised machine account.

Business Impact Description

If the Domain Controller is vulnerable, an attacker could authenticate to the domain as the Domain Controller and perform a DCSync attack to extract credentials for every domain account including Domain Admins. Exploitation of this vulnerability could lead to severe consequences, including threats to public safety, the compromise of internal APT corporate systems, and the exfiltration of sensitive information.

Affected Systems

The following systems in the internal.local domain are susceptible to the ZeroLogon vulnerability:

* 10.x.x.x – Desktop1 – Domain Controller

Finding Evidence

CENTRAL-05 used NetExec to identify machines vulnerable to ZeroLogon. Engineers found 3 machines, including a Domain Controller, that were vulnerable.

|  |  |
| --- | --- |
|  | NetExec smb ip -u ‘’ -p ‘’ -M zerologon |

/screenshot1

CENTRAL-05 did not exploit the vulnerability due to the potential risk of downtime.

Mitigations

* Install the August 11, 2020, Windows security updates on all vulnerable systems.
* Perform regular patch management and ensure devices are updated to mitigate security vulnerabilities.

References

* [**ZeroLogon WhitePaper**](https://cybersecurity.bureauveritas.com/blog/zero-logon)
* [**ZeroLogon Vulnerability Scanner**](https://github.com/SecuraBV/CVE-2020-1472)
* [**MSRC Netlogon CVE-2020-1472**](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472)
* [**Microsoft Mitigation Support Guide**](https://support.microsoft.com/en-us/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e)

**END OF FINDING BLOCK**