Advisory 2020-016

CVE-2020-1472 "Zerologon"– Netlogon Elevation of Privilege Vulnerability

The ACSC is aware of a recently disclosed critical vulnerability in Microsoft Active Directory Domain Controller systems that allows unauthenticated attackers to trivially access administrative credentials.

Proof of concept code to exploit the vulnerability is now freely available online and has been integrated into common exploit frameworks and tools.

CVE-2020-1472 also affects several other products not previously covered by the advisory, including, but not limited to:

- Samba implementations on Linux systems, prior to v4.8. This includes all Linux distributions that utilise the official Samba packages.

In most cases, CVE-2020-1472 is a privilege escalation vulnerability. However, adversaries may be able exploit the vulnerability for initial access if a Domain Controller is internet exposed.

ACSC recommended prioritised mitigations

The ACSC recommends organisations immediately patch affected Microsoft Windows systems with the Microsoft August 2020 Security Updates, released 11/08/2020. Where a security update cannot be immediately applied, the ACSC recommends organisations implement additional mitigations to prevent immediate exploitation. The ACSC recommends organisations ensure servers have completely applied the update, through a system reboot.

Where organisations cannot implement patching and hotfixes in a timely manner (such as in certain Critical Infrastructure environments), organisations should ensure logging is enabled for events documented below.

Organisations should ensure logging is enabled for the following events:

- **Event ID 4624**; **4742**– An account was successfully logged on, or A computer account was changed;
  - Events that contain the following fields should be assessed, and where possible diagnosed. Note that legitimate, legacy devices may utilise this functionality.
  - **Security ID: ANONYMOUS LOGON**
  - **Account Name: ANONYMOUS LOGON**
  - **Account Domain: NT AUTHORITY**

  Note: A computer account change *is not needed* for the exploit to be successful – It is possible for multiple exploits to be chained together to trigger this vulnerability without requiring Domain Controller password modification.

If a system is patched, monitor:

- **Event ID 5827**, **5828**, and **5829** – Events related to insecure connection attempts that are denied;
- **Event ID 5830**, and **5831** – Events related to insecure connection attempts that are successful.

More details of specific post-patch Event IDs are available in Microsoft's Mitigation Guidance.

ACSC recommended additional mitigations

Beyond the key mitigations above, the ACSC strongly recommends implementing the remainder of the ACSC Essential Eight Mitigation Strategies. Organisations that follow the ACSC's Essential 8 Mitigation Strategies and implement immediate system patching are protected from exploitation of this vulnerability. The ACSC recommends organisations verify that mitigations are applied. Microsoft has published specific security update details related to this vulnerability.

Due to the nature of this vulnerability, the ACSC recommends organisations at greater risk of exploit implement additional Defence-in-depth measures to ensure robust protection against exploitation. This vulnerability may allow adversaries to leverage external access for administrative domain credential compromise. Where external access is not possible, adversaries can utilise this vulnerability to trivially pivot throughout the target organisation's network once a device is compromised through other means, or introduced to the network.

1. Implement robust defence and detection measures at network boundaries, including:
   (a) Ensuring all administrative access protocols, ports, and Domain Controller access is not available externally, and where possible, not available via an organisations DMZ;
   (b) Most recent firewall products will be able to perform Deep Packet Inspection to detect network traffic that is attempting to exploit this vulnerability.
2. Implement additional protection mechanisms between domain controllers and user devices:
   (a) Domain controllers should be actively defended from untrusted devices;
   (b) Domain controller logs demonstrating documented activity should be immediately assessed for vulnerability or compromise.
3. Enable "**Enforcement Mode"** immediately:
   (a) Microsoft's Change Management Guidance provides details for organisations to implement "Enforcement Mode" immediately;
   (b) All legacy or non-compliant devices should be assessed, and eliminated from the network where possible.

Incident reporting

If you have questions about this advice or have indications that your environment has been compromised, contact the ACSC or calling 1300 CYBER1 (1300 292 371).

Becoming an ACSC Partner

The ACSC encourages all eligible organisations to become an ACSC Partner. As a partner, you will automatically receive threat intelligence, consisting of context-rich, actionable and timely information in a variety of formats, including advisories and automated indicator sharing.