Introduction

On 14 July 2020 (United States EST), Microsoft acknowledged a critical remote code execution (RCE) vulnerability existing in Windows Domain Name System (DNS) when it fails to properly handle requests. An adversary who successfully exploits the vulnerability could run arbitrary code in the context of the Local System Account.

The Australian Cyber Security Centre (ACSC) strongly recommends users apply the security patch to their Windows DNS Servers to prevent an adversary from exploiting this vulnerability.

The CVE-2020-1350 vulnerability - Critical

This vulnerability is being tracked as CVE-2020-1350 and has been assigned a CVSS base score of 10. The vulnerability is considered 'wormable' meaning it has the potential to spread between vulnerable devices without user interaction. As DNS is commonly installed on Domain Controllers, exploitation of this vulnerability could have a significant impact on organisational networks and services.

Microsoft has advised there are no mitigations available for this vulnerability, other than applying the security patch. For organisations that are unable to immediately apply the patch, Microsoft has supplied a registry modification workaround. Further information is available https://support.microsoft.com/en-us/help/4569509/windows-dns-server-remote-code-execution-vulnerability

If these options are unavailable or the workaround actions cannot be completed immediately, the ACSC recommends closely monitoring your Windows DNS Server and logs for any unusual activity.

Affected products and versions

The vulnerability, affecting the SigWireRead function, is known to be present in Windows DNS Server versions 2003 to 2019. The full list of affected versions and the associated Microsoft Knowledge Bulletins can be found at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

What do I need to do?

The ACSC strongly recommends organisations review KB4569509: Guidance for DNS Server Vulnerability CVE-2020-1350 for more information and apply the supplied critical security patch as soon as possible.

The ACSC recommends prioritising the security patch over implementation of individual mitigations. When applying security patches, the ACSC recommends prioritising external facing systems, followed by internal systems.

Patched versions of the affected components are available at Microsoft Support: CVE-2020-1350 | Windows DNS Server Remote Code Execution Vulnerability.

Further information

- MITRE CVE-2020-1350
- KB4569509: Guidance for DNS Server Vulnerability CVE-2020-1350
- CVE-2020-1350 | Windows DNS Server Remote Code Execution Vulnerability
- US-CERT CISA: Microsoft Addresses 'Wormable' RCE Vulnerability in Windows DNS Server