National Cyber Security Centre

2007141649-NCSC

A part of **Department of Communications, Climate Action & Environment**

NCSC Flash Alert

Microsoft Windows DNS Server Remote Code Execution
(CVE-2020-1350)
2020-07-14

Status: TLP-WHITE

NCSC

Threat Type	Check Point security researchers have recently discovered a critical 'wormable' vulnerability in Windows DNS Server which has a CVSS base score of 10.0. The full analysis from Check Point can be found here. Microsoft have issued an update on the vulnerability here. The flaw is in the way the Windows DNS server parses an incoming DNS query, and in the way it parses a response to a forwarded DNS query. If triggered by a malicious DNS query, it triggers a heap-based buffer overflow, enabling the hacker to take control of the server. Non-Microsoft DNS Servers are not affected. The NCSC strongly recommend users apply the patch to their affected under-support Windows DNS Server versions from 2008 to 2019 to prevent the exploitation of this vulnerability.
Products Affected	This vulnerability affects all Microsoft DNS Server versions 2003 to 2019.
Impact	If successfully exploited, it would give an attacker Domain Administrator rights over the server, and compromise the entire corporate infrastructure.
Recommendations	The NCSC strongly recommend users to patch their affected Windows DNS Servers in order to prevent the exploitation of this vulnerability. Patches are available from https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350.

Workaround	As a temporary measure until the patch is applied, the following registry modification has been identified as a workaround:
	
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\`
	`DWORD = TcpReceivePacketSize`
	`Value = 0xFF00`
	Note: A restart of the DNS Service is required to take effect.
	
	To remove the workaround:
	After applying the patch, the admin can remove the value TcpReceivePacketSize and its corresponding data so that everything else under the key
	
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters`
	
	remains as before.