NCSC
National Cyber Security Centre

2010141019-NCSC

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

NCSC Flash Alert

Windows TCP/IP Remote Code Execution Vulnerability
(CVE-2020-16898)
2020-10-14

Status: TLP-WHITE

NCSC

Threat Type	As part of its Patch Tuesday updates, Microsoft have released details of a remote code execution vulnerability that exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. More details can be found here.
Products Affected	The vulnerabilities affects a number of different versions of Microsoft Windows 10 and Microsoft Windows Server. The full list of affected products can be found here.
Mitigations	Microsoft has not identified any mitigating factors for this vulnerability.
Workarounds	NCSC-IE recommends that affected organisations should apply the appropriate updates or workarounds as recommended by Microsoft as soon as possible. Microsoft have recommended the following workaround: **Disable ICMPv6 RDNSS** • You can disable ICMPv6 RDNSS, to prevent attackers from exploiting the vulnerability, with the PowerShell command below. This workaround is only available for Windows 1709 and above. See here for more information. – **netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable** – **Note:** No reboot is needed after making the change. • To disable the workaround use the following PowerShell command: – **netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=enable** – **Note:** No reboot is needed after making the change.