National Cyber Security Centre

2102100250-NCSC

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

# NCSC Flash Alert

## Windows TCP/IP Remote Code Execution & DoS Vulnerabilities
## 2021-02-10

**Status:** TLP-WHITE

*This document is classified using Traffic Light Protocol. Recipients may share* TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

| | |
|---|---|
| **Threat Type** | Microsoft have released details of three important vulnerabilities, two Remote Code Execution (RCE) vulnerabilities (CVE-2021-24074, CVE-2021-24094) and a Denial of Service vulnerability (CVE-2021-24086).<br><br>• **CVE-2021-24074, CVSS 9.8(Critical)** - This is an Remote Code Execution (RCE) bug in Windows systems. An attacker could exploit this vulnerability by crafting traffic using **IP Fragmentation**, breaking a packet into multiple fragments and reassembling on the endpoint, or by using **Loose Source and Record Route (LSRR)**, "Source Routing", a way for packets to request routers to choose and record the path through which the network will route them.<br><br>• **CVE-2021-24094, CVSS 9.8 (Critical)** - Under certain circumstances, when tcpip.sys performs a "recursive reassembly" on fragmented packets, the reassembly process can cause the driver to leave open a pointer to memory space that has been de-allocated, which can be exploited to remotely execute code.<br><br>• **CVE-2021-24086, CVSS 7.5(High)** - This vulnerability exists when Windows tcpip.sys driver attempts to reassemble fragmented IPv6 packets. As a result, this attack requires many packets to be successful. The root cause of this vulnerability is a NULL pointer de-reference which occurs in Ipv6pReassembleDatagram. The crash occurs when reassembling a packet with around 0xffff bytes of extension headers. Microsoft regard this vulnerability as easier for attackers to exploit so taking action quickly is recommended.<br>Please review Microsoft's Release Notes for Patch Tuesday February 2021: https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb. |
| **Products Affected** | Multiple Microsoft Products |
| **Impact** | Remote Code Execution & Denial of Service |
| **Recommendations** | Please install the patches supplied by Microsoft as quickly as possible. It is expected, that because of the the elevated risk with these vulnerabilities, exploits will be developed by attackers in the near future. |

**DISCLAIMER:** *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
**Tel:** +353 (0)1 6782333
**Mail:** certreport@decc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie