National Cyber Security Centre

22041301000-NCSC

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

NCSC Alert

Multiple Critical Vulnerabilities in Microsoft Products CVE-2022-24491, CVE-2022-24497, CVE-2022-26809

2022-04-13

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.*

Description

The NCSC is highlighting some critical vulnerabilities which have been included in Microsoft's monthly patch Tuesday release. The CVE's highlighted in this alert include Remote Code Execution vulnerabilities where exploitation has been assessed as being *"more likely"*[1] by Microsoft.

- **CVE-2022-24491 & CVE-2022-24497 CVSSv3: 9.8 (Critical) - are both Windows Network File System (NFS) Remote Code Execution Vulnerabilities** - that affect systems that have the NFS role enabled. An attacker could send a specially crafted NFS protocol network message to a vulnerable Windows machine, which could enable remote code execution. More information can be found here:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24497
- **CVE-2022-24497 CVSSv3: 9.8 (Critical)- Remote Procedure Call Runtime Remote Code Execution Vulnerability** - an attacker could send a specially crafted RPC call to an RPC host. This could result in remote code execution on the server side with the same permissions as the RPC service. More information can be found here:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809

Products Affected

Multiple Microsoft Windows systems, full details of affected products can be found at the following link:
https://msrc.microsoft.com/update-guide/releaseNote/2022-Apr

Recommendations

Organisations should apply the monthly security updates as per Microsoft guidance. The NCSC would also advise that as a rule, services on **TCP port 445 should not be exposed to the Internet**. However, should an attacker gain access to a network through other means (successful spearphish etc.) failing to patch this vulnerability will provide a significant lateral movement capability to the attacker, potentially enabling unfettered network access. Perimeter hardware and appliance firewalls that are positioned at the edge of the network should block unsolicited communication (from the internet) and outgoing traffic (to the internet) to the following ports:

- SMB - TCP - **445**
- NetBIOS Name Resolution - UDP - **137**
- NetBIOS Datagram Service - UDP - **138**
- NetBIOS Session Service - TCP - **139**

The use of NetBIOS for SMB transport ended in Windows Vista & Windows Server 2008, and in all later Microsoft operating systems when Microsoft introduced SMB 2.02. However, you may have software and devices other than Windows in your environment. You should disable and remove SMB1 if you have not already done so because it still uses NetBIOS. Later versions of Windows Server and Windows no longer install SMB1 by default and will automatically remove it if allowed.

[1] https://www.microsoft.com/en-us/msrc/exploitability-index?rtc=1

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