National Cyber Security Centre

2107011010-NCSC

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

NCSC Alert

Microsoft Windows Print Spooler RCE Vulnerability - CVE-2021-34527 UPDATE 2021-07-07

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.*

Revision History

Revision	Date	Author(s)	Description
1.0	01 July 2021	CSIRT-IE	Initial Alert created regarding new Print Spooler Vulnerability affecting Microsoft Windows.
1.1	02 July 2021	CSIRT-IE	Additional information from Microsoft, including the assignment of CVE-2021-34527 and link to Microsoft guidance
1.2	07 July 2021	CSIRT-IE	Updated to include details about patch released by Microsoft

Threat Type	The NCSC are aware of a Remote Code Execution (RCE) vulnerability, along with Proof of Concept (PoC) code for the Microsoft Windows Print Spooler service **(CVE-2021-34527)**. This vulnerability can allow an authenticated, remote attacker to gain SYSTEM privileges by sending an RpcAddPrinterDriverEx() RPC request in all versions of Windows. The RpcAddPrinterDriverEx() function is used to install a printer driver on a system. Any authenticated user can call RpcAddPrinterDriverEx() loading a driver file locally or from a remote system. By leveraging the vulnerability, the Print Spooler Service, spoolsv.exe, executes code in an arbitrary DLL file with SYSTEM privileges. Microsoft released a patch for CVE-2021-34527. CSIRT-IE strongly recommend that all organisations examine the advice from Microsoft.
Products Affected	All versions of Microsoft Windows
Impact	Remote Code Execution - compromised systems, data loss.
Recommendations	Microsoft released a patch on 6th July 2021. Please refer to the Microsoft guidance regarding this vulnerability. The updates do not include Windows 10 version 1607, Windows Server 2012, or Windows Server 2016—Microsoft states updates for these versions are forthcoming. Microsoft has also provided workarounds in case the patch cannot be applied. (**Please Note**, these workarounds will need to be evaluated before being applied to your environment.): • Disable the Print Spooler service to prevent exploitation. (Disabling the Print Spooler service disables the ability to print both locally and remotely.) • Disable inbound remote printing through Group Policy. Computer Configuration / Administrative Templates / Printers, **Disable** the **"Allow Print Spooler to accept client connections:"** policy to block remote attacks. Security researchers have published research and provided workarounds available if disabling the Print Spooler is not an option. • This blog post from Truesec offers a potential mitigation by restricting Access Control Lists. • Lares Labs, a security consulting company published a repository with detection and remediation information. • Florian Roth, a security researcher, has released experimental Sigma Rules for detecting exploitation of the vulnerability.

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