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
2021-07-01

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

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 has stated that this vulnerability is similar but distinct from the vulnerability that is assigned CVE-2021-1675, which addresses a different vulnerability in RpcAddPrinterDriverEx(). The attack vector is different as well. CVE-2021-1675 was addressed by the June 2021 security update. There is **not** currently a patch available for CVE-2021-34527.
Products Affected	All versions of Microsoft Windows
Impact	Remote Code Execution - compromised systems, data loss.
Recommendations	Please refer to the Microsoft guidance regarding this vulnerability: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527. Currently, there are no patches available for this vulnerability, the following workarounds have been suggested (**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. • If disabling the Print Spooler is not an option, the following 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, based off of one the publicly available PoCs. For information regarding possible side-effects of disabling system services please see the following guidance from Microsoft.

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