One Solution. One Company.

SN-10

CVE-2021-34527 (Print Nightmare) Vulnerability

Version 1.0.0

1 Overview

The CVE-2021-34527 vulnerability, known as 'Print Nightmare,' affecting the Windows spooler service, was disclosed on June 9th, 2021 [1]. This document offers a concise overview of the 'Print Nightmare' and its implications for IDIS products.

2 What is ‘Print Nightmare’?

‘Print Nightmare' is a bug in the Windows spooler service that, under certain circumstances, allows an attacker to remotely execute code on a Microsoft Windows system as the local SYSTEM user [2].

This vulnerability potentially grants hackers elevated administrator privileges, enabling them to remotely control your PC, install malware and ransomware, and access or destroy sensitive data without physical access to the computer [3].

'Print Nightmare' affects all versions of the Windows print spooler, including those installed on personal computers, enterprise networks, servers, and domain controllers [3].

3 Impacts of ‘Print Nightmare’ on IDIS Products

3.1 Standalone Products: NVRs, DVRs and IP Cameras

IDIS standalone products use the Linux OS and are not affected by this vulnerability.

3.2 Windows OS based Products

IDIS has the following Windows OS based products and these products are affected by this vulnerability.

(1) For IR-100, IR-300(A), DV-2232, DV-3100, ID29/39xx: Windows Embedded Standard (WES) 8, 64-bit

The Windows print spooler will not accept client connections by default. However, if an authorized user shares out a local printer or opens the print queue on a printer connection, the Windows print spooler will begin accepting client connections and become exposed to this vulnerability.

(2) IR-1100: Windows Server 2016 or Windows 10, 64bit

The Windows print spooler will be activated and exposed to this vulnerability.

(3) IR-1000: WES 8 or Windows Server 2012 R2, 64bit

The Windows print spooler will be activated and exposed to this vulnerability.

(4) IDIS Center or IDIS Solution Suite: Depending on user server’s Windows OS

If the spooler service is not disabled by the user, the Windows printer spooler will be activated and exposed to this vulnerability.

Please take one of the following actions to protect your products from this vulnerability.

(1) Download and install the patch software corresponding to the installed Windows OS. (Recommended)

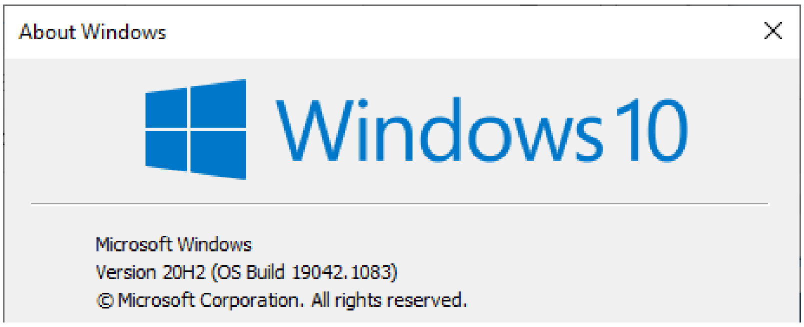
- WES 8 OS: KB5004956 Windows patch software
- Windows Server 2016 OS: KB5004948 Windows patch software

  : Same as Windows 10's KB5004948 patch software
- Windows 10 OS or other OSs : Please refer to the '**Updates**' section of the MSRC > Customer Guidance > Security Update Guide > Vulnerabilities > CVE 2021 34527 [4].

  After confirming the Windows OS name and version used in your product, please download and install the appropriate patch software.

  You can check the Windows OS name and version by using the following command.

  ■ Press 'Windows (⊞) + R' keys, enter '**winver**' into the 'Run' dialog box, and then click 'OK'.



About Windows

Microsoft Windows
Version 20H2 (OS Build 19042.1083)
© Microsoft Corporation. All rights reserved.

- Option) Please refer to the following websie if you want to view installed patch software for Windows.

  https://forums.ivanti.com/s/article/How-To-View-Installed-Updates-for-Windows-Using-WMIC?language=en_US

(2) Disable the print spooler service

- Please refer to **Workaround** section of the MSRC > Customer Guidance > Security Update Guide > Vulnerabilities > CVE 2021 34527 [4].

(3) Disable inbound remote printing through Group Policy

- Please refer to **Workaround** section of the MSRC > Customer Guidance > Security Update Guide > Vulnerabilities > CVE 2021 34527 [4].

Contact Us

Additional information may be updated in this document in the future. For any questions or concerns related to this issue, please email security@idisglobal.com.

References

[1] https://cve.mitre.org/

[2] https://www.papercut.com/kb/Main/PrintNightmareCVE2021#what-is-print-nightmare

[3] https://eminetracanada.com/how-to-avoid-windows-print-nightmare-security-threats/213364/

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Version History

Version	Writer	Revision Date	Remarks
1.0.1	Daniel Lee	Jul. 13. 2021	Initial Release