

Project Vulnerability Description ReporT

CVE-2021-1675

ICT287 Computer Security



Thien Twee Zian

34664971

**Table of Contents**

[Introduction 2](#_Toc139390478)

[Discovery of CVE-2021-1675 2](#_Toc139390479)

[Importance of CVE-2021-1675 4](#_Toc139390480)

[Demonstration of Vulnerability 5](#_Toc139390481)

[Mitigation 6](#_Toc139390482)

[Conclusion 6](#_Toc139390483)

[Appendix 7](#_Toc139390484)

[Vulnerability Details : CVE-2021-1675 (Details 2022) 7](#_Toc139390485)

[Shodan Search (Shodan 2022) 8](#_Toc139390486)

[Flowchart to indicate the exploitability of PrintNightmare across various platform configurations (Dormann 2021) 9](#_Toc139390487)

[References 10](#_Toc139390488)

# Introduction

CVE-2021-1675, also called PrintNightmare, is an Elevation of Privilege Vulnerability that specifically focuses on the Windows Print Spooler application activated by default on all Windows-based systems. Exploiting this vulnerability enables an attacker with limited access privileges to construct and employ a malicious DLL file, which by doing so, the attacker can execute an exploit and attain elevated privileges.

CVE-2021-1675, also referred to by the same name, resembles CVE-2021-34527. Nevertheless, they differ in terms of their nature. While 1675 is categorized as a privilege elevation vulnerability, 34527 is classified as a remote code execution (RCE) vulnerability. In the context of this report, our focus will solely be on CVE-2021-1675.

# Discovery of CVE-2021-1675

On June 8, 2021, Microsoft released the "Microsoft June 2020 Patch Tuesday update" patch to address CVE-2021-1675. The discovery of this vulnerability is credited to several researchers, including Zhipeng Huo from Tencent Security Xuanwu Lab, Piotr Madej from AFINE, and Yunhai Zhang from NSFOCUS TIANJI Lab.

**Blast radius**

CVE-2021-1675, as reported by the National Institute of Standards and Technology's Vulnerability Database, holds a CVSS score of 9.3 out of 10 (Technology 2022). This high score can be attributed to several factors;

1. Widespread Impact: The vulnerability affects the Windows Print Spooler, a core component of the Windows operating system that is enabled by default on all Windows-based systems. This wide distribution increases the potential attack surface and the number of systems that could be affected.
2. Privilege Elevation: CVE-2021-1675 is classified as a privilege elevation vulnerability. This means that an attacker with low access privileges can exploit the vulnerability to gain higher privileges on the compromised system. Privilege escalation can significantly impact the security posture of a system, allowing an attacker to gain unauthorized access to sensitive data or perform unauthorized actions.
3. Ease of Exploitation: Exploiting CVE-2021-1675 does not necessarily require complex techniques or sophisticated tools. An attacker with basic knowledge and skills can craft and utilize a malicious DLL file, potentially leading to privilege elevation. The relative ease of exploitation increases the likelihood of successful attacks and raises the severity of the vulnerability.
4. Potential for Lateral Movement: By gaining elevated privileges through CVE-2021-1675, an attacker can move laterally within a network, potentially compromising additional systems and expanding their control and access. This lateral movement capability amplifies the overall impact of the vulnerability.

Considering the combination of widespread impact, the potential for remote code execution, and ease of exploitation, the CVSS score for CVE-2021-1675 is assessed as high to reflect its significant security risks.

More details about the CVSS score and the products affected by it can be found in the appendix.

# Importance of CVE-2021-1675

Windows continues to maintain its position as the most prevalent operating system (OS) today. As per data from Shodan, a specialized search engine for identifying and retrieving information about internet-connected devices, this OS has over 14 million recorded users. This emphasizes the significance of CVE-2021-1675, as it impacts numerous versions of Windows and highlights the severity of the vulnerability due to its extensive reach across a wide range of affected systems.

Exploiting this vulnerability grants attackers access to administrative rights, allowing unauthorized retrieval of sensitive data. Furthermore, attackers can install backdoors to establish persistent access to the target system, enabling them to maintain control and carry out malicious activities over an extended period.

The ease of exploiting this vulnerability is indeed a significant concern. The availability of tutorials on platforms like YouTube and readily accessible exploit codes on GitHub further exacerbate the situation. These resources provide malicious actors with step-by-step instructions and pre-written code, making launching successful attacks on exposed systems easier. This widespread availability of information increases the risk of exploitation and highlights the importance of promptly addressing vulnerabilities and securing systems against potential attacks.

# Demonstration of Vulnerability

For demonstrating an exploit of CVE-2021-1675, I will be using a code from GitHub, specifically the CVE-2021-1675 - PrintNightmare LPE (PowerShell) by Caleb Stewart and John Hammond (Stewart and Hammond 2021). The target would be a Windows 10 system, version 1909.

A local user account would be created on the target system to simulate a local actor carrying out the attack. A copy of the script would be downloaded from the GitHub source and saved. From there, a PowerShell would be used to run the script, with the intended result of creating a new administrative account, with username "adm1n" and password "P@ssw0rd" as the default setting. The script can also be altered to set the username and password to the attacker's choosing.

With access to the newly created admin account, the attacker would be free to carry out other actions, such as retrieving sensitive data, changing the rights of other users, etc.

More information about how the vulnerability is exploited can be found at <https://www.kb.cert.org/vuls/id/383432>.

# Mitigation

Updating the Windows OS to the latest version is recommended, as the vulnerability was patched back in June 2021.

Another method applicable is to disable the Print Spooler service, which can be done via the following command in PowerShell,

* Stop-Service -Name Spooler -Force
* Set-Service -Name Spooler -StartupType Disabled

# Conclusion

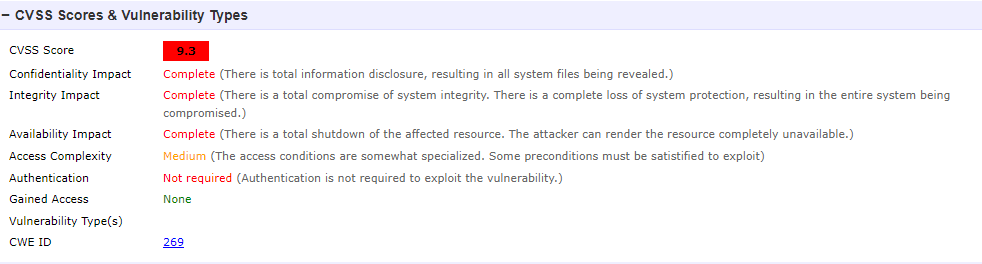
By examining the potential exploits associated with CVE-2021-1675, it becomes evident that vulnerabilities can be present even in default applications provided by major companies like Windows. This underscores the significance of regular updates to counter the ever-increasing occurrence of vulnerabilities in the wild.

Furthermore, understanding the ease with which this vulnerability can be exploited, coupled with the availability of accessible tools on the internet for novice users to learn and employ, emphasizes the importance of maintaining constant vigilance against such threats. It is crucial to recognize that these threats can originate from various sources, including disgruntled employees within an organization who may lack prior experience but possess the intention to cause harm.

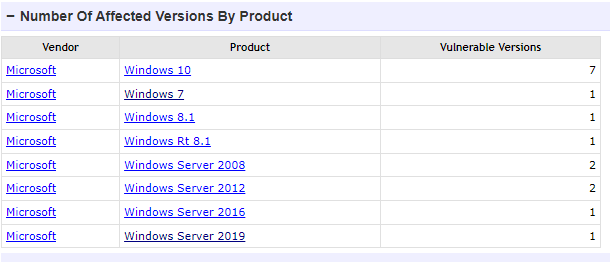
# Appendix

## Vulnerability Details : CVE-2021-1675 (Details 2022)

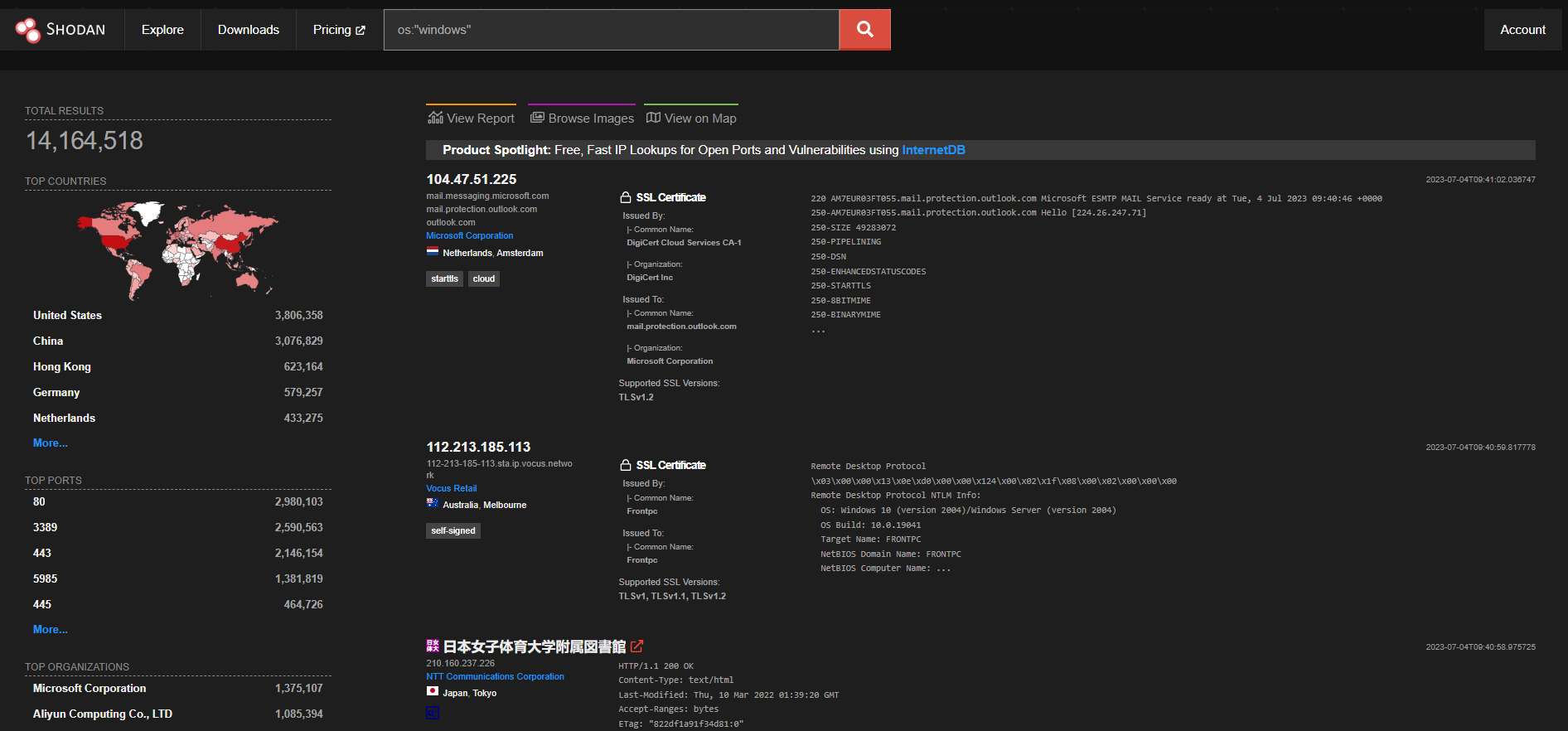
From <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2021-1675>



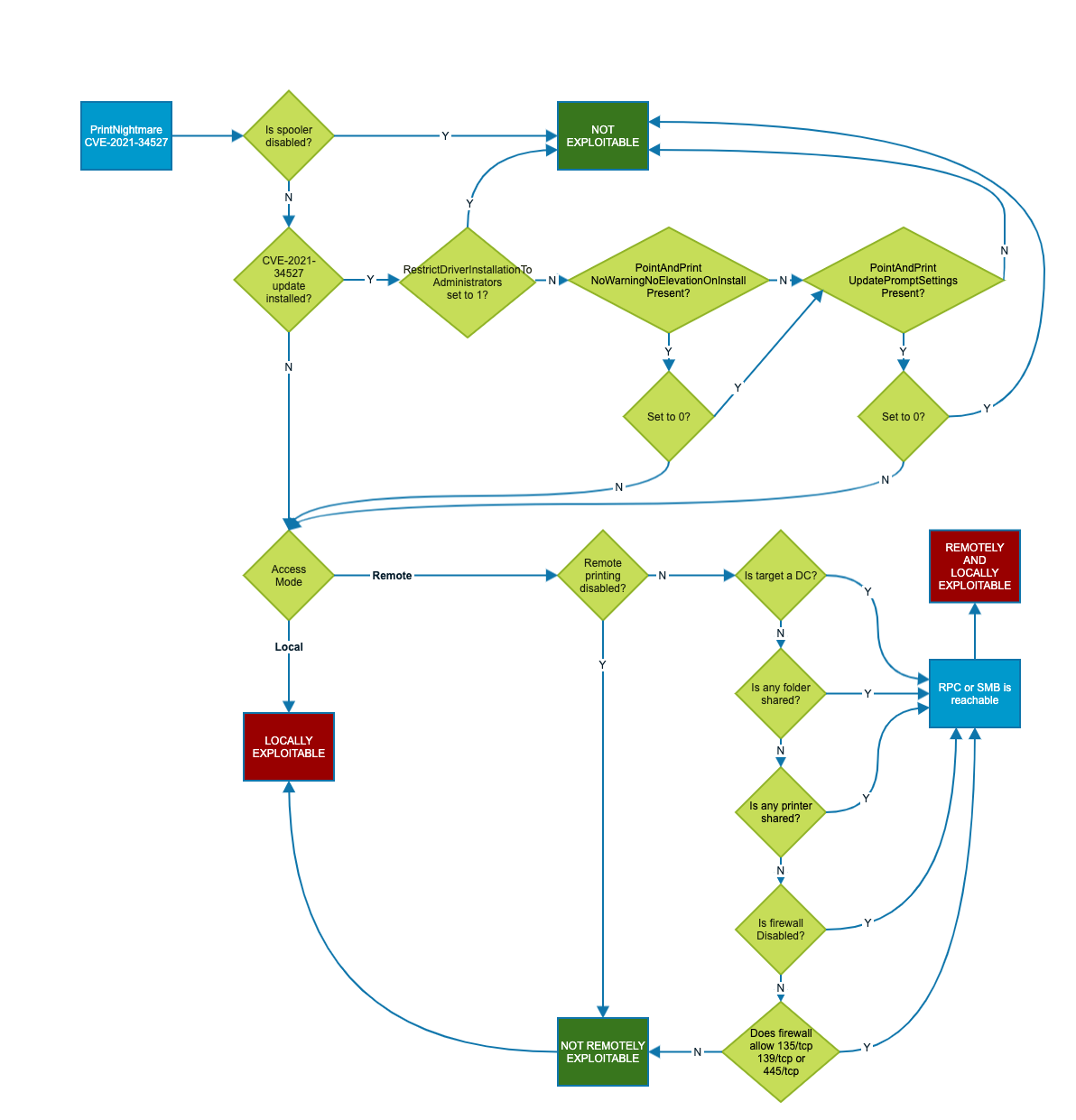




## Shodan Search (Shodan 2022)



## Flowchart to indicate the exploitability of PrintNightmare across various platform configurations (Dormann 2021)



# References

Details, C. (2022). "Windows Print Spooler Elevation of Privilege Vulnerability." from <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2021-1675>.

Dormann, W. (2021). "Microsoft Windows Print Spooler allows for RCE via AddPrinterDriverEx()." from <https://www.kb.cert.org/vuls/id/383432>.

Lab, K. (2021). "Quick look at CVE-2021-1675 & CVE-2021-34527 (aka PrintNightmare)." from <https://securelist.com/quick-look-at-cve-2021-1675-cve-2021-34527-aka-printnightmare/103123/>.

Lab, K. (2021). "A Windows Print Spooler vulnerability called PrintNightmare."

Laskowski, B. (2021). "PrintNightmare (CVE-2021-1675 and CVE 2021-34527) Explained." from <www.blumira.com/cve-2021-1675/>.

MiniTool (2022). "What Is Print Spooler and How to Reset It on Windows 10? [MiniTool Wiki]."

Rapid7 (2021). "CVE-2021-34527 (PrintNightmare): What You Need to Know." from <https://www.rapid7.com/blog/post/2021/06/30/cve-2021-1675-printnightmare-patch-does-not-remediate-vulnerability/>.

Shodan (2022). "Shodan Search on Windows OS." from <https://www.shodan.io/search?query=os%3A%22windows%22>.

Stewart, C. and J. Hammond (2021). "CVE-2021-1675 - PrintNightmare LPE (PowerShell) ". from <https://github.com/calebstewart/CVE-2021-1675>.

Technology, N. I. o. S. a. (2022). "CVE-2021-1675 Detail." from <https://nvd.nist.gov/vuln/detail/CVE-2021-1675>.

Tills, C. (2021). "CVE-2021-1675: Proof-of-Concept Leaked for Critical Windows Print Spooler Vulnerability." from <https://www.tenable.com/blog/cve-2021-1675-proof-of-concept-leaked-for-critical-windows-print-spooler-vulnerability>.