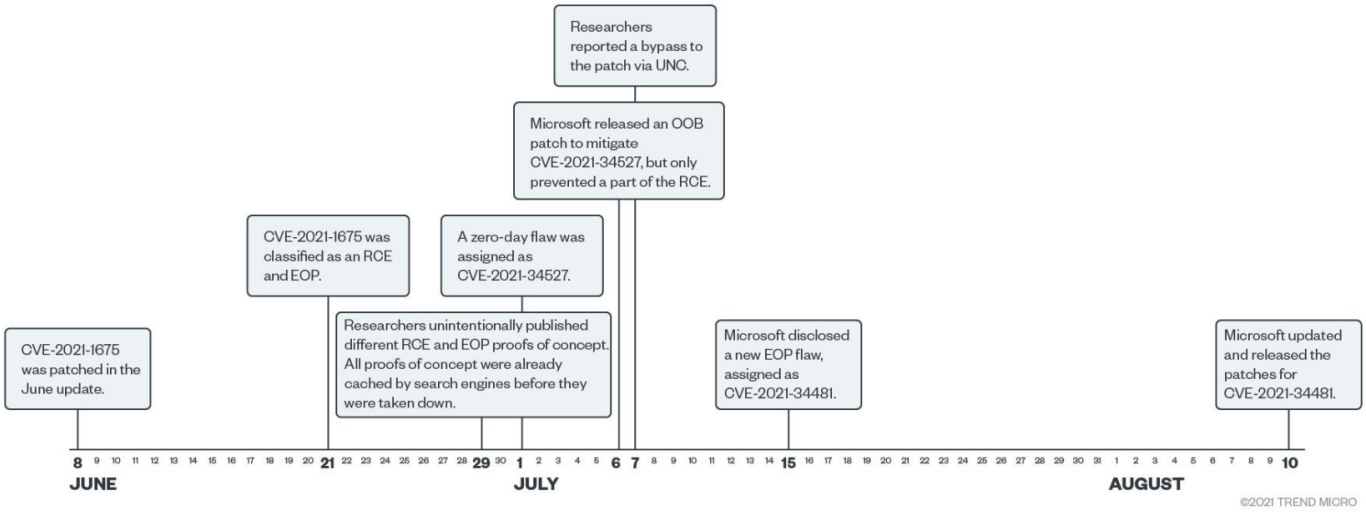
Print Nightmare - Attaque des spooler d'impression

Historique



Description

PrintNightmare: Understand and Overcome

In June of 2021, Microsoft issued a warning entitled “Windows Print Spooler Remote Code Execution Vulnerability.” This vulnerability, known as PrintNightmare, leaves the print spooler open for a hacker to attack by allowing anyone to remotely install a printer ‘driver’ with the ability to execute malicious code and take complete control of a PC. The attacker could access data, create new accounts, and destroy users' accessibility to their devices.

This is an ongoing issue. While there has been a security update from Microsoft addressing this vulnerability, it is not perfect, and many devices are still at risk. We will discuss ways to mitigate the problem and keep devices safe from this vulnerability. By following the steps in this post, you will be better equipped to handle these attacks and reduce the probability of becoming the next victim.

What is the Print Spooler?

The print spooler service is a software program that manages any print jobs that need to be sent to a printer server. In many cases, Microsoft relies on this program for the organization and control of its devices. It is an essential program for anyone needing to print, and it keeps the print jobs organized and in order. While the print spooler is a practical and often necessary tool, it can also be dangerous if it falls into the wrong hands.

Some of the most basic functions of a print spooler include:

- Managing the files that are in the process of printing on the device
- Monitoring the files that are in the process of printing on the device
- Keeping everything in order and organized as the items print

Most Microsoft machines have the print spooler system automatically enabled, and many do not think twice about it when activating their device for the first time. After all, when hackers are not attempting to break into it, it can be a very beneficial (and often necessary) tool.

Since its original release, there have been few maintenance updates on the print spooler. It was this lack of improvement that could have left it vulnerable to hackers and attackers. However, in July 2021, Microsoft issued a security update addressing this vulnerability. They are recommending that users install these updates immediately. After all, you do not want to be the next company with a data security breach.

Understanding the PrintNightmare Vulnerability

The PrintNightmare vulnerability first appeared in a June 2021 release by two research teams. It was so named because of the versatile nature of this weakness across a variety of different products. Recently, the PrintNightmare shifted from 'low' severity to 'critical' severity. Users need to be aware of this as it grows worse.

To fully understand this vulnerability, it is important to be familiar with the print spooler and how attackers can use it to their advantage. This issue is a critical flaw that may need to be handled in-house while Microsoft works towards finding a permanent solution for all users. Otherwise, the system could be taken over by hackers.

What Are the Vulnerabilities in the System?

Two central vulnerabilities lie inside of the print spooler system. Each serves as a different attack point for a hacker trying to find a way into vulnerable devices. It is critical to understand each of them so that you know the weak points that they target.

The core vulnerabilities include:

- Local privilege escalation, ensuring that a hacker who gets into a computer with low privilege can elevate to an admin level on the device
- Remote code execution, which can allow the systems to be weaponized either locally or by using a domain controller

These vulnerabilities can offer power to the attackers that allow them to take over many systems at once.

How Can Hackers Use This to Their Advantage?

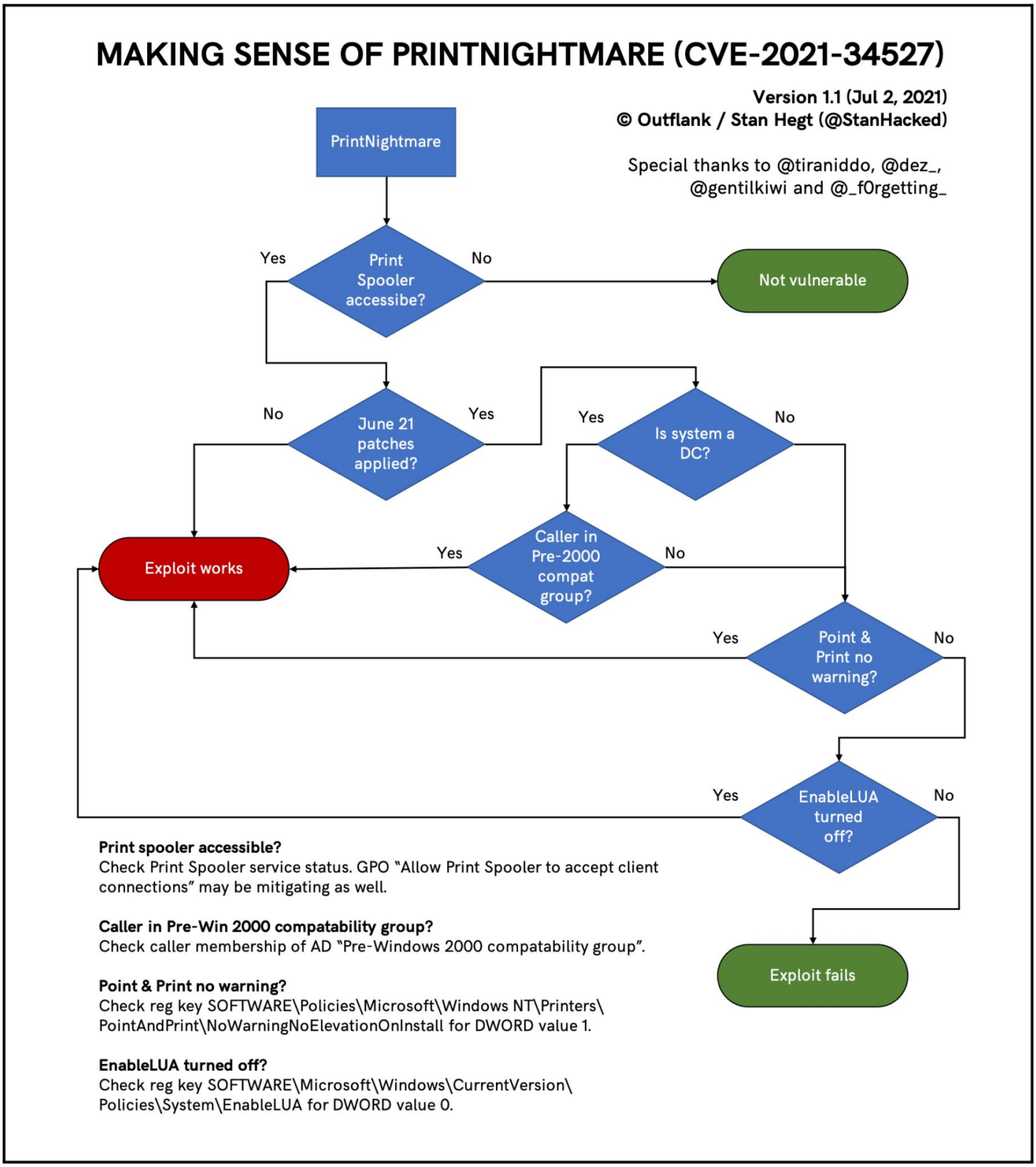
It can be a little bit difficult to understand what hackers can do with access to a print spooler. This device's only job is to manage printing items and does not seem like it would be very threatening. It is a program that many people overlook, yet hackers can pose a massive threat if they gain access to this software.

This threat includes:

- Hackers gaining access to sensitive information
- Manipulating private and personal data to their advantage
- Installing malicious programs onto the device

These are just a few of the things that can happen if an attacker gains control of a system through the print spooler. It can be a massive invasion of privacy.

Schéma



Sources

https://msandbu.org/printnightmare-cve-2021-1675/

https://www.edgenetworks.us/blog/understanding-printnightmare-a-print-spooler-vulnerability

https://www.trendmicro.com/fr_fr/research/21/h/detecting-printnightmare-exploit-attempts-with-trend-micro-vision-one-and-cloud-one.html

---

Revision #1
Created 2026-07-17 15:09:51 UTC by Olivier
Updated 2026-07-17 15:09:54 UTC by Olivier