Microsoft

Microsoft Out-Of-Band Security Release

July 6, 2021

Agenda

- Security Update
- Additional Resources

Overview – Print Spooler Vulnerability

- All supported versions of Windows
- CVE-2021-34527 was updated to include fixes
- Limited, targeted attacks detected
- Today’s update is cumulative. It includes the June 2021 security updates.

CVE-2021-34527 Print Spooler

Impact, Severity, Disclosure

Remote Code Execution | Critical | Publicly disclosed | Exploitation detected

CVSSScoreMetrics

Base CVSS Score: 8.8 | Attack Vector: Network | Attack Complexity: Low | Privileges Required: Low | User Interaction: None

Mitigations

Microsoft has not identified any mitigating factors for this vulnerability

Workarounds

Option 1: disable the Print Spooler service.
Option 2: disable inbound remote printing through GPO
See Security Update Guide for details.

Affected Software

Server, version 20H2
Server, version 2004
Server 2019
Windows 10
Server 2016
Server 2012 R2
Server 2012
Windows 8.1

Frequently Asked Questions

Is this the vulnerability that has been referred to publicly as PrintNightmare?

Yes, Microsoft has assigned CVE-2021-34527 to this vulnerability.

Is this vulnerability related to CVE-2021-1675?

This vulnerability is similar but distinct from the vulnerability that is assigned CVE-2021-1675. The attack vector is different as well. CVE-2021-1675 was addressed by the security update released on June 8, 2021.

Did the June 2021 update introduce this vulnerability?

No, the vulnerability existed before the June 8, 2021 security update.

All versions of Windows are listed in the Security Updates table. Are all versions vulnerable?

All versions of Windows are vulnerable. Supported versions of Windows that do not have security updates available on July 6 will be updated shortly after July 6.

FAQ continued

What vulnerabilities do the security updates released on and after July 6, 2021 address?

The security updates released on and after July 6, 2021 contain protections for a remote code execution exploit in the Windows Print Spooler service known as “PrintNightmare”, documented in CVE-2021-34527, as well as for CVE-2021-1675.

Are Domain Controllers known to be affected by the vulnerability?

Domain controllers are affected if the print spooler service is enabled.

Are client systems and member servers that are not domain controllers known to be affected by the vulnerability?

Yes. All supported editions of Windows are affected.

How can I see attack activity on my network related to this vulnerability?

Security products, like Microsoft 365 Defender, offer different ways to view relevant alerts and telemetry. Microsoft has published our recommendations for seeing this sort of behavior at our GitHub here: Microsoft 365 Defender Hunting Queries. Customers using other technologies can adapt this logic for use in their environments.

FAQ continued

How is Point and Print technology affected by this particular vulnerability?

Point and Print is not directly related to this vulnerability, but the technology weakens the local security posture in such a way that exploitation will be possible. To harden Point and Print make sure that warning and elevation prompts are shown for printer installs and updates. These are the default settings but verify or add the following registry modifications:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
NoWarningNoElevationOnInstall = 0
NoWarningNoElevationOnUpdate = 0
```

We also recommend explicitly listing specific print servers which should be used by clients.

For more information see:

Introduction to Point and Print - Windows drivers | Microsoft Docs

Use Group Policy settings to control printers - Windows Server | Microsoft Docs

Policy CSP - Printers - Windows Client Management | Microsoft Docs

Defender Protections

Microsoft Defender Antivirus

Trojan:Win32/Priteshel.A
Trojan:Win32/Priteshel.B
Detection version 1.343.229.0 or higher

Resources

Microsoft 365 Defender Hunting Queries

https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/tree/master/Exploits/Print%20Spooler%20RCE

KB5005010: Restricting installation of new printer drivers after applying the July 6, 2021 updates

https://support.microsoft.com/help/5005010

Microsoft

Questions?