Olympus Winter & Ibe GmbH, Kuehnstraße 61, 22045 Hamburg

To whom it may concern

Date
30.07.2021

PrintNigthmare -
Windows Print Spooler Remote Code Execution Vulnerability

Dear Sirs and Madams,

A critical vulnerability in the Windows Print Spooler Service was detected. It was called “Print-Nightmare". Microsoft assigned the number **CVE-2021-1675** to this vulnerability.

On June 29, 2021, exploits for the vulnerability began circulating. Microsoft assigned a second number to this vulnerability: **CVE-2021-34527**.

On 7 July 2021 Microsoft released out-of-band updates for some (but not all) versions of Windows. According to Microsoft's updated advisory, "the security updates released on and after July 6, 2021 contain protections for CVE-2021-1675 and the additional remote code execution exploit in the Windows Print Spooler service known as “PrintNightmare”, documented in CVE-2021-34527." Exploitation in the wild has been detected, and ALL Windows systems are affected.

On July 15, 2021 Microsoft assigned a third number to the PrintNightmare vulnerability: **CVE-2021-34481**. There is no known public exploit for this vulnerability yet.

Affected OSTE devices

All versions of the following OSTE products include a version of Windows and are affected by the PrintNightmare vulnerability:

- VMC-3
- VMC-7
- VMC-10
- VMC-30.

OSTE released Service Bulletin SBU_100-219-293 to address the PrintNightmare vulnerability on these products. This Service Bulletin contains instruction for the service engineers, how to stop and disable the Print Spooler Service in Windows for VMC-3, VMC-7, VMC-10, and VMC-30. Disabling the Print Spooler Service of Windows is a quick and effective solution to close the PrintNightmare vulnerability in Windows.

Contact the Olympus service to have the remediation actions defined in Service Bulletin applied on your VMC.

Other OSTE products

OSTE also produces and delivers software, that must be installed on computers running Windows as operating system:

- ENDOBASE
- Hytrack

Due to the high risk of the PrintNightmare vulnerability, OSTE strongly recommends to apply the following remediation instructions in order to minimize the risk caused by the PrintNightmare vulnerability.

General Recommendation

Affected from the PrintNightmare vulnerability are all Windows versions and all types of Windows – clients and server installations.

If a Windows computer does not need the print functionality, OSTE recommends to stop and disable the Print Spooler Service of Windows on these computers. Disabling the Print Spooler Service remediates the PrintNightmare Vulnerability on all versions and types of Windows. But it also disables the possibility to print from a computer.

The print functionality is required for Hytrack servers if automatic printing of reprocessing protocols should be done and on Hytrack clients for manual printing of protocols.

On ENDOBASE servers the print function is not necessary.

For the third CVE number associated with PrintNightmare – CVE-2021-34481 – disabling the Print Spooler Service is the only workaround given by Microsoft at the date of the release of this document (July 2021).

More information is available at the Microsoft web page for CVE-2021-34481:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

If printing from a Windows Computer is required, the recommended remediation action depends on the Windows version.

Windows 10 and Windows 10 based Server Versions

Microsoft published security updates for all versions of Windows 10 and the related server versions. Detailed information and links to the related knowledgebase articles are available at the Microsoft web page for CVE-2021-34527:

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

In addition to installing the updates, to secure your system, you must confirm that the following registry settings are set to 0 (zero) or are not defined:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)`
- `UpdatePromptSettings = 0 (DWORD) or not defined (default setting)`

Having `NoWarningNoElevationOnInstall` set to 1 makes your system vulnerable by design.

Windows 7 and Windows 7 based Server Versions

Microsoft published security updates for Windows 7 and Windows 7 based Server versions only for customers with an Extended Support Update (ESU) contract.

If disabling the Print Spooler Service is no option, there are only some workarounds to minimize the risk created by the PrintNightmare vulnerability.

Disable inbound remote printing through Group Policy

Configure the settings via Group Policy as follows:

`Computer Configuration / Administrative Templates / Printers`

Disable the "`Allow Print Spooler to accept client connections`" policy to block remote attacks.

You must restart the Print Spooler service for the group policy to take effect.

Detailed information is available at the Microsoft web page for CVE-2021-34527:

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

Restricting installation of new printer drivers (Point and Print settings)

Also, without an installed security update the following settings are recommended to mitigate the risk created by the PrintNightmare vulnerability:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)`
- `UpdatePromptSettings = 0 (DWORD) or not defined (default setting)`

Having `NoWarningNoElevationOnInstall` set to 1 makes your system vulnerable by design.

Kind regards

Alois Baier
Product Security Manager
R&D | Product Security