Product Security Bulletin

Important Information - Please Read and Keep

Subject: “PrintNightmare” Security Vulnerability

Date: 2021-07-07 (last update)
Originator: Timo Kosig

Background

Microsoft has disclosed a remote code execution vulnerability which has been named “PrintNightmare” (CVE-2021-34527) in the Windows Printer Spooler service affecting its Windows operating systems (for a complete list please review the linked Microsoft bulletin).

What PrintNightmare does

The vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

The vulnerability has a CVSS 3.0 Base Score of **8.8 (high)**.

Microsoft has stated that exploitations of the vulnerability have been detected.

Response

Affected Vyaire Products

Any Vyaire product running a Microsoft Windows operation system is potentially affected.

How Microsoft Is Responding

Microsoft has issued an Out-of-band (released outside of regular schedule) security update that has been announced in the Windows message center on the Microsoft website.

Microsoft recommends that customers update their devices as soon as possible.

Mitigations & Compensating Controls

Vyaire recommends its customers to install the appropriate out-of-band security update for their Windows operating system as soon as possible. The update has been tested for compatibility with Vmax™ and SentrySuite® 3.20, 3.10, 3.0 and 2.21.

If installation of the update is not immediately possible, Vyaire recommends utilizing the workaround "Option 2" as described by Microsoft in the vulnerability bulletin. This workaround will prevent remote exploitation of the vulnerability:

> **Option 2 - Disable inbound remote printing through Group Policy**
>
> You can also 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.
>
> **Impact of workaround** This policy will block the remote attack vector by preventing inbound remote printing operations. The system will no longer function as a print server, but local printing to a directly attached device will still be possible.

Vyaire does not recommend completely disabling the Windows Printer Spooler service as this will break our products' ability to generate PDF reports and printed reports and will lead to application malfunctions.

Generic controls

- Ensure your data has been backed up and stored according to your individual process and that your disaster recovery procedures are in place.
- Update your anti-virus and malware protection, where available.

For product or site-specific concerns, contact your Vyaire service representative.

For more information on Vyaire's proactive approach to product security and vulnerability management, contact us at productsecurity@vyaire.com or visit www.vyaire.com/product-security.

Timo Kosig
timo.kosig@vyaire.com
Product Security Leader
Vyaire Medical