Product Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

CVE-2020-601 Microsoft Windows Security Vulnerability

Date: 2020-01-22

Background

The NSA has discovered a certificate validation security vulnerability in a cryptographic library used by Microsoft Windows 10 and Windows Server 2016 and 2019. (NSA Cybersecurity Advisory).

Microsoft has published patches to remediate this vulnerability. (CVE-2020-0601)

What The Vulnerability Does

An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider.

A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.

What Operating Systems Are Affected

Affected operating systems include Microsoft Windows 10, Windows Server 2016 and Windows Server 2019.

Other Windows operating systems are not affected by the vulnerability.

Details regarding the vulnerability and the Microsoft's impacted products and responses may be found here and here.

Response

How Microsoft Is Responding

Microsoft communicated the issue to its customers on January 14th 2020. Microsoft recommends that all affected systems are patched as soon as possible. Patches have been made available to download.

Affected Products

Vyaire's medical devices affected include all Windows-based respiratory products which use an affected operating system.

Vyaire has tested all affected products for compatibility with the patches and has found **no** issues. **Vyaire recommends installing the patches as soon as possible.**

Mitigations & Compensating Controls

Ensure that the patches made available by Microsoft have been applied to the operating system of your computers:

Windows 10, Windows Server 2016 and 2019: Microsoft Advisory CVE-2020-0601, published January 14th 2020.

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 under: http://www.vyaire.com/productsecurity

GLOBAL HEADQUARTERS

Vyaire Medical, Inc.
26125 North Riverwoods Blvd
Mettawa, IL 60045
USA