Product Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

BlueKeep Security Vulnerabilities

Date: 2019-05-21 **DocumentID: SEC-04**

Background

A security vulnerability in the Remote Desktop Protocol (RDP) known as **BlueKeep** (CVE-2019-0708) has received significant news coverage for its potential impact.

What BlueKeep Does

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

What Operating Systems Are Affected

Affected operating systems include Microsoft Windows XP, Windows 7 SP1, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2.

Windows 8 and Windows 10 are **not** affected by BlueKeep.

Details regarding the vulnerability and the Microsoft's impacted products and responses may be found here. Proof of Concept exploit code has been authored but is not yet publicly available.

VYR-GBL-1900041

Product Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

Response

How Microsoft Is Responding

Microsoft has communicated the issue to its customers on May 14th 2019. Microsoft strongly recommends that all affected systems are patched as soon as possible. Patches have been made available to download – also for Windows XP and Windows Server 2003 which no longer receive mainstream support.

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 to install 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 7, Windows Server 2008: Microsoft Advisory CVE-2019-0708, published May 14th 2019
- Windows XP, Windows Server 2003: Microsoft Customer guidance for CVE-2019-0708, published May 14th 2019

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

VYR-GBL-1900041