Product Security Bulletin

Important Information - Please Read and Keep

Subject: CVE-2021-21551 Security Vulnerability

Date: 2021-05-17 (last update)

Originator: Timo Kosig

Background

Security researchers have found five high severity flaws in Dell's firmware update driver (summary). The vulnerability CVE-2021-21551 (National Vulnerability Database) can affect a broad range of Dell's laptops, desktops, notebooks and tablets.

What CVE-2021-21551 does

Dell's ***dbutil_2_3.sys*** driver contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required.

The vulnerability has a CVSS 3.1 Base Score of **8.8 (high)**.

The driver is packaged by Dell as part of a range of different Dell Client firmware update utility packages and tools.

Response

Affected Vyaire Products

The Dell PCs or laptops that are used with Vyaire's respiratory diagnostics medical devices **have not been shipped** with any of the vulnerable Dell Client firmware update utility packages and tools.

Therefore, **no medical devices** manufactured by Vyaire are directly affected by CVE-2021-21551.

However, customers may have installed this driver file on their Windows operating system when they used firmware update utility packages, Dell Command Update, Dell Update, Alienware Update, Dell System Inventory Agent, or Dell Platform Tags, including when using any Dell notification solution to update drivers, BIOS, or firmware for their system.

How Dell Is Responding

Dell has communicated CVE-2021-21551 to its customers in the security advisory made available on their website.

The security advisory clearly outlines remediation steps on how to remove the affected driver file from the system.

Mitigations & Compensating Controls

Vyaire recommends its customers to check that the affected driver file is not installed on any of their Dell PC systems.

If the file is found, Vyaire recommends to follow the remediation steps as outlined in Dell's security advisory.

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