FRESENIUS

"BLUFFS" Statement

Publication date: 2024 April 10

This document aims to provide information on the assessment of a potential product impact linked with the disclosed vulnerability "BLUFFS".

Executive Summary

As detailed in the research-paper released by EURECOM[1], a cybersecurity vulnerability has been found on Bluetooth BR/EDR devices with Secure Simple Pairing and Secure Connections pairing in Bluetooth Core Specification 4.2 through 5.4. This vulnerability allows certain man-in-the-middle attacks by forcing a short key length. This might lead to the discovery of the encryption key and live injection of data. The MITRE Corporation assigned the CVE ID CVE-2023-24023[2] to this vulnerability. Furthermore, NVD[3] evaluated its overall CVSS score as 6.8 which is considered medium.

This vulnerability could concern medical devices which utilize the Bluetooth protocol stack to communicate data. According to the Bluetooth SIG[4]:

> *"If a reduced encryption key length can be negotiated, the MITM attacker may be able to brute force the encryption key by trial and error to permit decryption of the traffic between devices. As the same encryption key can be forced by the MITM for all encryption establishment while in proximity to the impacted peer devices if that encryption key can be brute forced, all prior and subsequent attacked sessions are also vulnerable to being decrypted. The recommended minimum encryption key length for BR/EDR encrypted sessions is 7 octets. Brute forcing of a 7-octet key is not anticipated to be possible in real-time during a session, however, an attacker able to co-locate with attacked devices may be able to record sufficient private traffic to make an attack on a single session key worthwhile. If a successful attacker can reduce the encryption key length below 7 octets, the attacker may be able to complete a brute forcing of the encryption key in real-time, permitting live injection attacks on traffic between the affected peers. For this attack to be successful, an attacking device needs to be within wireless range of two vulnerable Bluetooth devices initiating an encryption procedure using a link key obtained using BR/EDR Secure Connections pairing procedures."*.

[1] https://dl.acm.org/doi/abs/10.1145/3576915.3623066
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24023
[3] https://nvd.nist.gov/vuln/detail/CVE-2023-24023
[4] https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/bluffs-vulnerability/

The Fresenius group is actively monitoring “BLUFFS”. Furthermore, analysis actions were taken to assess any potential impact on our products.

The following vulnerability is associated with “BLUFFS”:

- CVE-2023-24023

At date, impacted products have been assessed and no uncontrolled or unacceptable risks have been identified when considering products current design and intended use environment. Refer to below Fresenius assessment and impact analysis for details.

Fresenius products assessment

The following list of products were assessed and **are not affected by "BLUFFS"**.

Fresenius Kabi

Product	**Versions**
Infusion Pumps – Agilia	All versions
Infusion Pumps – Exelia	All versions
Enteral Nutrition Pumps – Amika	All versions
Infusion Pumps – INfusia	All versions
Enteral Nutrition Pumps – Enfusia	All versions
Vigilant Software Suite	All versions
Agilia Partner	All versions
Exelia Partner	All versions
Amika Partner	All versions
INfusia Centro	All versions
KabiHelp Pro	All versions
Aurora	All versions
Aurora Xi	All versions
AmiCORE	All versions
Amicus	All versions
Phelix	All versions
Alyx	All versions
Lovo	All versions
Cue	All versions
CATSmart	All versions
COM.TEC	All versions
CompoDock	All versions
CompoGuard	All versions
CompoMat G5	All versions
CompoSeal Mobilea II	All versions
CompoSeal Slim	All Versions
Infusion Pump - Ivenix	All Versions

The following list of products was assessed and **are affected:**

Fresenius Kabi

Product	**Versions**
Conox Device	All versions

BLUFFS impact rationale for not affected products

The listed products are not using the Bluetooth protocol.
None of "BLUFFS" reported vulnerability can be exploited on these products.

BLUFFS impact analysis for CONOX

General impacts (according to research paper)

The BLUFFS attacks could have a severe impact on Bluetooth's security and privacy. They allow decrypting (sensitive) traffic and injecting authorized messages across sessions by re-using a single session key. Prior attacks require leaking pairing key or brute-forcing one session key per target session to achieve a similar impact. This attack can target any Bluetooth device, regardless of its role, security mode, and supported Bluetooth profiles, as they rely on flaws in the standard. Moreover, the attacks are stealthy since they exploit the Bluetooth firmware (Controller) without requiring user interaction and triggering notifications to the user. Finally, the attacks do not require specialized and expensive equipment, and have a widespread impact.

Potential impacts on Conox

- **Conox QM7000-M (FW4.10):** Legacy pin, it can likely be attacked by MitM trough BLUFFS.
- **Conox 2D (FW5.10)**: Secure simple pairing set to «Just Work », it can likely be attacked by MitM trough BLUFFS.
- **Conox DtC (FW5.40):** Secure simple pairing set to «Pairing Key Confirmation », it can likely be attacked by MitM trough BLUFFS. The complexity of the attack might be higher due to enhanced security settings.

The risks when Conox is attacked are:

- Bluetooth data sent from the Conox can be stolen
  Existing risk control measure or compensating controls:
  - *No personal data are sent, only EEG and Anesthesia Indexes.*

  - *Attacker needs to know or decodify the communication protocol in order to find the meaning of the data on the stream (proprietary structure – non standard).*
  - *If the attack causes that data are not yet received on ConoxView on remote device, a warning message is displayed, user can detect it.*
- Incorrect or large amount of data can be sent to Conox by the attacker
  Existing risk control measure or compensating controls:
  - *Conox does not read data from Bluetooth, only uni-directional communication, no impact on anesthesia indexes or anesthetic monitoring operations.*
  - *In case of denial of service, if Bluetooth crashes, there is no impact on device essential performance. Data will not be received on ConoxView remote device, a warning message will be shown to the user.*
- Incorrect or fake data can be sent to external device on ConoxView
  Existing risk control measure or compensating controls:
  - *Attacker needs to know or decodify the communication protocol in order to find the meaning of the data on the stream (proprietary structure – non standard).*
  - *ConoxView performs an integrity check: An attacker needs to recalculate CRC on modified data packets and send the new CRC in the correct position of the data frame, otherwise data will be ignored.*
  - *ConoxView intended use is not for monitoring purpose, only data displayed on Conox device shall be used for that purpose.*

Additionally, the statement from Microchip (supplier of Bluetooth chip) is:

> "*The BLUFFS vulnerability is not affecting the RN4678. The attack is under BR/EDR Secure Connections enabled, but BM78/RN4678 doesn't support BR/EDR Secure Connections feature.*"

Residual Risk Rationale for Conox

- The Conox device has been designed to prevent the communication layer from disturbing the anesthetic monitoring layer.
- Any potential Denial of Service attack will only affect the communication layer, not the anesthetic monitoring layer.
- Hence, in case of Bluetooth crash or communication loss, the device will keep functioning and the monitoring of patient is not interrupted.
- Important to mention that the Conox device does not read the data from the Bluetooth interface, but only transfer data from the device to the external application through the Bluetooth interface.
- As such, it is not possible to leverage any buffer overflow vulnerability to gain privileged access to the device, take control of the device or modify the data that are displayed on the device.
- In case of communication interruption between the Conox device and the external device, the main functionality of the Conox device is not affected, hence with no impact on patient monitoring. Only the remote display external application software ConoxView, that is installed on the external device, would be affected by a loss of communication that would be warned on the user interface.
- In case of data modification during the transmission (Communication interception, Man-in-the-Middle Attack), ConoxView might display fake or

incorrect data. However, ConoxView intended use is not for monitoring purpose, only data displayed on Conox device shall be used for that purpose.

Conclusion for Conox

An attack trough BLUFFS vulnerability exploitation on the Conox device does not affect patient safety and will not leave to unacceptable disruptions of the data transmitted over Bluetooth communication interface. Compensating risk control measures exist, cybersecurity recommendations are also present in the product accompanying document to remind end-users about best practices and physical security policies to apply in the intended used environment.

Hence, a patching correction on the Conox device is not considered as urgent. The vulnerability is monitored through applicable medical device cybersecurity post-market events and incidents handling procedure.

- Update of the Conox device version already in the market previous to Conox 2024 release is not taken into account as they will be progressively replaced by new 2024 version.
- Regarding Conox 2024 release, when a patch will be made available for the Bluetooth module RN4678, it will be analyzed and implemented.

BLUFFS Cybersecurity recommendations for impacted product

- Conox device users shall ensure the products are installed and used as intended according to the products accompanying documentation recommendations.

General Cybersecurity recommendations

Proper cybersecurity hygiene and behavior is required to safely integrate Medical Devices into IT infrastructure. The Fresenius Group recommends operators of Medical Devices and software to incorporate the following industry best practices into their defense-in-depth strategy:

- Conduct a comprehensive and periodic security risk assessment on the medical network in accordance with operational security best practices such as IEC 80001-1 and ISO 27002
- Minimize network exposure for all medical devices and systems, and ensure that they are not accessible from the Internet
- Locate Fresenius Medical Devices behind firewalls, in dedicated medical networks, isolated from all other IT networks
- Monitor and control access and traffic to the dedicated medical network
- Implement application firewalls capable of deep packet inspection to help protect against zero-day vulnerabilities and the latest exploits
- Use appropriate authentication and authorization of users on the network
- Implement physical controls that ensure no unauthorized persons would have access to the medical devices and systems
- Ensure that all programming software and equipment (service laptops, etc.) are kept in locked cabinets and are never connected to any network other than the medical network they are intended to service
- Ensure that all portable media used for data exchange with the medical network (such as CDs, USB drives, etc.) are scanned before use
- Implement a process to monitor, prevent and contain malwares and computer viruses.

Institutionalizing strong cybersecurity policies and following the industry best practices relative to IT security could minimize exposure to threats. These threats may include but not limited to: Data Leak, Data Corruption, Data Loss, Network or Service Outage, etc.

References

Regarding “BLUFFS” more details can be found on:
EURECOM research-paper: https://dl.acm.org/doi/abs/10.1145/3576915.3623066
Bluetooth SIG: https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/bluffs-vulnerability/
MITRE Corporation: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24023

Contacts

For any questions or suggestions please contact your regional marketing manager.