Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

WPA2 "KRACK" Wi-Fi Vulnerability

Date: 2019-03-08 **DocumentID: SEC-02-180926**

Background

Vyaire is monitoring the situation around a set of vulnerabilities found in the WPA2 protocol which is used to secure communications between a Wi-Fi enabled client device and a Wi-Fi access point. The vulnerabilities may affect confidentiality, integrity, and availability of communication between an access point and client devices such as a computer, phone, Wi-Fi base stations, and other gear, even though the connection is encrypted. This is NOT a Vyaire-specific vulnerability, but could affect any Wi-Fi devices that use the WPA2 protocol.

This set of vulnerabilities has been called Key Reinstallation attACKs (KRACK), which if exploited can allow an attacker to manipulate data traffic between device and access point which results in partial disclosure of encrypted communication or injection of data into it. In order to successfully exploit the vulnerability the attacker needs to be within physical range of an affected Wi-Fi access point and client. This vulnerability potentially affects all business industries including the healthcare industry.

There are currently no reported verified instances of the KRACK vulnerability being exploited maliciously against medical devices; however, if KRACK is successfully exploited in a healthcare environment, it is anticipated that affected hospital networks could experience unauthorized patient record changes and/or disclosure and major IT disruptions. To prevent such issues, remediating KRACK will require a series of actions to be taken by the IT Department in healthcare facilities and vendors on which Vyaire depends.

Response

Affected Products

Please note that a number of Vyaire products utilize third-party vendor technologies, which create an interdependence between Vyaire patch deployment processes and third-party vendors' patch releases. The following list shows Vyaire products that may reside on wireless networks that could be vulnerable to KRACK:

- V-178501 Vyaire Vyntus WALK (Dell Venue 7 TC01 Android Tablet)
- V-178501 Vyaire Vyntus WALK (Asus Nexus 7 Android Tablet)
- V-178501 Vyaire Vyntus WALK (Samsung SM-T280 Android Tablet)
- 30343-001 Vyaire Ventilator Wireless Bridge for AVEA ventilators

Vyaire Vyntus WALK

KRACK can be exploited from an adjacent network however the attack complexity is high as it requires proximity to an affected Wi-Fi access point and significant technical skills. No privileges or user interaction is required to exploit this vulnerability. The scope is unchanged while both confidentiality and integrity are rated high as KRACK causes complete loss of control over unencrypted data. There is no availability impact.

The calculated CVSS base score is 6.8 (medium).
The CVSS vector string is CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Vyaire Ventilator Wireless Bridge

KRACK can be exploited from an adjacent network however the attack complexity is high as it requires proximity to an affected Wi-Fi access point and significant technical skills. No privileges or user interaction is required to exploit this vulnerability. The scope is unchanged while confidentiality, integrity and availability impact are rated “none”.

The Ventilator Wireless Bridge is vulnerable to CVE-2017-13078 and CVE-2017-13080 and while these vulnerabilities possibly allow an attacker to replay broadcast frames that are sent from the

Wi-Fi access point to a client device our review of our application has concluded that the Ventilator Wireless Bridge is not affected by that scenario.

The calculated CVSS base score is 0.0 (none).
The CVSS vector string is CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N

Mitigations & Compensating Controls

Vyaire Vyntus WALK

Google has provided patches for the KRACK vulnerability in Android through the 2017-11-06 security patch level. Neither Google, Dell nor Samsung have issued firmware updates for the affected tablets and are unlikely to do so in the future.

Vyaire recommends its customers to mitigate the vulnerability by employing either one of the following compensating controls:

- Disabling Wi-Fi on the tablet and connect to SentrySuite by using USB tethering and a USB cable (please see the user manual)

  - OR -

- Configuring SSL encryption for traffic between the Vyntus WALK Android application and SentrySuite (please contact your Vyaire service representative)

Either control will fully mitigate the vulnerability's effect on confidentiality and integrity and reduce the CVSS base score to 0.0.

Vyaire Ventilator Wireless Bridge

The manufacturer of the Wi-Fi module used in the Ventilator Wireless Bridge will not provide a firmware update to mitigate the existing vulnerabilities. Vyaire is currently reviewing the possibility to change the Wi-Fi module used as part of a standard product sustaining process to ensure that newly sold devices are not vulnerable anymore.

The Ventilator Wireless Bridge is by default configured to not listen to broadcast frames that are sent from the Wi-Fi access point.

The Ventilator Wireless Bridge may be reconfigured by other personnel than Vyaire's field service representatives (e.g. customer's IT department).

When changing the configuration it is important to ensure that Vyaire's application of the Ventilator Wireless Bridge is not affected by the vulnerabilities (please see the user manual for details):

- Check that the function **UDP Receiver** is disabled (**Service** tab of the configuration utility)
- Check that the **Address** of the remote peer is configured as a TCP connection (**Client** tab of the configuration utility)

If a customer has other devices from other vendors that share the same network then these devices may be affected if they are susceptible to replay of broadcast frames if the aforementioned vulnerabilities are exploited.

Vyaire therefore recommends its customers to put Vyaire ventilators on a dedicated Wi-Fi network that is not shared with other (medical) devices.

Generic controls

Vyaire also recommends the following for Wi-Fi enabled networks and clients to minimize risk and impact:

- Ensure the latest recommended updates from device manufacturers have been installed
- Ensure appropriate physical controls are in place
- Ensure data has been backed up and stored according to your individual processes and disaster recovery procedures

VYR-GBL-1900003

Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

For additional technical details and indicators associated with this vulnerability, review US-CERT Vulnerability Note VU#228519

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-1900003