Product Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

Ransomware Activity Targeting the Healthcare and Public Health Sector

Date: 2020-10-30 (last update)

Background

Vyaire Medical is aware of and monitoring the situation of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers, as published by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) in their alert AA20-302A warning.

What Ransomware does

Ransomware is a type of malware that encrypts computer data/storage and then attempts to extort money from the victim in exchange for access to the data decryption key, notably with limited historical success of decryption.

Ransomware infections typically begin with social engineering attacks - such as phishing - targeting employees: the employee receives a maliciously crafted email, opens the attachment or link and while doing so infects his/her device, which then spreads on the organization's network.

Response

How the CISA Is Responding

The CISA has released a detailed threat alert which includes technical background information on the types of ransomware involved, mitigation plans and best practices to follow in order to avoid and limit spread of a ransomware infection.

How Vyaire Is Responding

Vyaire will continue to monitor the ongoing situation. Vyaire recommends its customers to keep operating systems updated with recent security patches made available by Microsoft and to follow mitigations as outlined by CISA in the respective threat alert and in the CISA Ransomware Guide (published September 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.

Information on disaster recovery procedures

In case a Vyaire product has been affected by a ransomware attack please contact your Vyaire service representative for assistance with disaster recovery procedures.

Disaster recovery will involve restoring systems from an existing customer backup and comes with different levels of complexity depending on product and the extent of the systems affected that will need to be restored.

Exemplary disaster recovery procedures for SentrySuite based respiratory diagnostics products

SentrySuite stand-alone systems

Stand-alone SentrySuite systems can be either restored from a bare-metal backup or from a backup of the SentrySuite SQL database. If only a SQL database backup is available, the reinstallation of the Windows OS and the SentrySuite application will be required as well as restoring the SQL database.

SentrySuite client systems

SentrySuite client systems can be restored directly from a bare-metal backup. If not available, the Windows OS must be reinstalled as well as the SentrySuite client application.

Since SentrySuite stores all application configuration data in the central SQL database the client system's configuration may be restored directly from the central database once SentrySuite has been reinstalled.

SentrySuite client systems and application backend server

Should both SentrySuite client workstation systems and the application backend server have been affected then a staged disaster recovery process is required:

Application Backend Server:

1. Re-install the operating system on the application backend server
2. Install and set up MS SQL Server on the application backend server
3. Restore the SentrySuite SQL database on the application backend server from a backup
4. Install SentrySuite on the application backend server and configure it to use the restored SQL database

SentrySuite client workstations:

1. Re-install the operation system on all affected SentrySuite client workstation PCs
2. Install SentrySuite on all client PCs
3. Restore existing workstation configuration from the central database through SentrySuite

For other product or site-specific concerns, please 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

GLOBAL HEADQUARTERS

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

Vyaire Medical GmbH
Leibnizstrasse 7
97204 Hoechberg
Germany

AUSTRALIAN SPONSOR

Vyaire Medical Pty Ltd
Suite 5.03, Building C
11 Talavera Road
Macquarie Park, NSW, 2113
Australia

CE 0123

Rx ONLY For global distribution.