Product Security Bulletin

Important Information - Please Read and Keep

Subject: SentrySuite™ – SQL Injection and Authenticated Remote Code Execution vulnerabilites

Date: 2022-12-20 (last update)
Originator: Timo Kosig

Background

Vyaire proactively communicates with our customers to inform them about cybersecurity issues to help healthcare delivery organizations identify and remediate potential cybersecurity risks.

This bulletin contains product security information and recommendations related to two cybersecurity vulnerabilities that Vyaire identified within its SentrySuite™ software.

Response

Affected Vyaire Products

Vyaire has confirmed that the following versions of its SentrySuite™ software are affected by the vulnerabilities found:

- SentrySuite™ 3.20 (up to and including Maintenance Package 5)

Vyaire is currently reviewing the status of the following SentrySuite versions which are still under active support by Vyaire:

- SentrySuite™ 3.10
- SentrySuite™ 3.0

This bulletin will be updated with further information as it becomes available.

Affected Product Components

Vyaire SentrySuite™ software offers two different deployment options, SentrySuite™ can either be deployed as a client-server application with a dedicated application backend server, or as a stand-alone application.

Please see the following table to identify which product components are affected depending on the chosen deployment scenario.

Deployment mode	Vulnerability	
	SQL Injection	Authenticated Remote Code Execution
Stand-alone	Only if connected to the network	Only if connected to the network
Client-server	Yes, only application backend server is affected, clients are not affected	Yes, only application backend server is affected, clients are not affected

Vulnerability Details

SQL Injection

The SentrySuite™ application backend server and SentrySuite™ installed as a stand-alone system are vulnerable to a SQL Injection attack. Vyaire Product Security has analyzed the vulnerability and has assigned the following CVSS score to this vulnerability:

CVSS: 8.3 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Authenticated Remote Code Execution

The SentrySuite™ application backend server and SentrySuite™ installed as a stand-alone system are vulnerable to an Authenticated Remote Code Execution attack. Vyaire Product Security has analyzed the vulnerability and has assigned the following CVSS score to this vulnerability:

CVSS: 8.2 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Mitigations & Compensating Controls

Vyaire recommends implementing the following mitigations and compensating controls to reduce risk associated with these vulnerabilities:

For customers running SentrySuite™ 3.20 (up to and including Maintenance Package 5)

- Install SentrySuite™ 3.20 Maintenance Package 6 which fully remediates both vulnerabilities. Please contact your Vyaire field service representative or get in touch via the Vyaire website to schedule installation.

For customers running SentrySuite™ 3.10 or 3.0

- For client-server deployments
  - Please follow the generic controls described in the next section.
- For network-connected stand-alone deployments:
  - Ensure that the host-based firewall is enabled on the computer system and is configured correctly for your usage. SentrySuite ™ does not require any open incoming ports in stand-alone mode in a default configuration. Usage of electronic interfaces to hospital information systems, electronic medical record systems or other systems must be evaluated separately.

Generic controls that should be considered in all scenarios

The following generic controls are recommended by the document *Vyaire Product Security White Paper - SentrySuite 3.20 V1* which is available to all customers upon request:

- 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 Manager
Vyaire Medical GmbH

Holger Schmitt
holger.schmitt@vyaire.com
Senior Product Manager Software and IT integration
Vyaire Medical GmbH

GLOBAL HEADQUARTERS

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