PRODUCT SECURITY BULLETIN

Important information - Please read and keep

JAEGER

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

Date: 2023-05-17 (last update)

Background

We proactively communicate 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 we have identified within SentrySuite™ software.

Response

Our Affected Products

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

SentrySuite™ 3.20 (up to and including Maintenance Package 6)
SentrySuite™ 3.10 (up to and including Maintenance Package 8)
SentrySuite™ 3.0 (up to and including Maintenance Package 10)

Affected Product Components

The 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

For Global Distribution.

Vulnerability Details

SQL Injection

The SentrySuite™ application backend server and SentrySuite™ installed as a stand-alone system are vulnerable to a SQL Injection attack. Product Security team has analysed 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. Product Security team has analysed 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

We recommend implementing the following mitigations and compensating controls to reduce risk associated with these vulnerabilities:

For customers running SentrySuiteTM 3.20 (up to and including Maintenance Package 6)

- Install SentrySuite™ 3.20 Maintenance Package 7 which fully remediates both vulnerabilities. Please contact your Jaeger Medical field service representative or get in touch via the Jaeger Medical website to schedule installation.

For customers running SentrySuite™ 3.10 (up to and including Maintenance Package 8)

- Install SentrySuite™ 3.10 Maintenance Package 9 which fully remediates both vulnerabilities. Please contact your Jaeger Medical field service representative or get in touch via the Jaeger Medical website to schedule installation.

For customers running SentrySuite™ 3.0 (up to and including Maintenance Package 10)

- Install SentrySuite™ 3.0 Maintenance Package 11 which fully remediates both vulnerabilities. Please contact your Jaeger Medical field service representative or get in touch via the Jaeger Medical website to schedule installation.

Generic controls that should be considered in all scenarios

The following generic controls are recommended by the document 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 Jaeger Medical service representative.

For more information on the Jaeger Medical proactive approach to product security and vulnerability management, contact us at productsecurity@jaegerrdx.com or visit www.jaegerrdx.com/product-security.