Product Security Bulletin

Important Information - Please Read and Keep

vyaire MEDICAL

Subject: Mirth Connect Security Vulnerabilities

Date: 2024-05-29 (last update)

Background

NextGen Healthcare Mirth Connect is an open-source integration engine used primarily in healthcare IT for exchanging healthcare data between various systems. It enables interoperability between different healthcare applications, and allows secure and efficient transfer of data through standardized protocols and formats such as HL7, DICOM, and FHIR.

IHTeam identified a remote command execution on Mirth Connect <= 4.3.0 that can be exploited from an unauthenticated perspective. The only condition in which this CVE can be exploited is when JRE <= 8.0 is in use. The vulnerability reportedly came as a side-effect of the company trying to fix a previous critical-severity flaw, tracked as **CVE-2023-37679**. This vulnerability, carrying a severity score of 9.8, was also described as a pre-auth remote code execution.

Later, researchers from Horizon3.ai determined the patch to be incomplete and published a gadget chain which bypassed the deny list that the original had implemented. This second vulnerability was assigned **CVE-2023-43208** and was patched in Mirth Connect version 4.4.1

Response

Affected Vyaire Products

The Vyaire SentryConnect solution, which is utilized to connect SentrySuite™ solutions to hospital information systems, utilizes Mirth Connect for integration purposes. Mirth Connect is **potentially** vulnerable to **CVE-2023-37679** and **CVE-2021-44228**.

How Vyaire Is Responding

Vyaire has implemented the below changes around the disclosure of the Mirth Connect vulnerabilities from **SentryConnect Gateway version 6.0.2.1** onwards.

- Removed legacy properties from mirth.properties file regarding encryption, digest and security,
- Added random strong passwords for keystore generation
- Removed deprecated https ciphersuites
- Updated MirthConnectAdminLauncher to version 1.4.1
- TLSv1.3 Support added
- TLSv1.1 Support removed
- Http socket on port 8080 permanently closed

- Upgrade to MirthConnect 4.4.1
- Upgrade to openJDK 17.0.4.1 (LTS)
- Upgrade MirthConnect's jetty 9.4.44 to jetty 9.4.49

Mitigations & Compensating Controls

Vyaire recommends to apply the following mitigations and compensating controls:

- Customers using versions before **SentryConnect Gateway version 6.0.2.1** have to reach out to **support.connect.eu@vyaire.com** to initiate the update process and also allow Vyaire support to make additional configurational changes

For product or site-specific concerns, contact your Vyaire service representative.

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