swisslog
healthcare

Swisslog Healthcare
11325 Main Street
Broomfield, CO 80020

800.764.0300
healthcare.us@swisslog-healthcare.com
swisslog-healthcare.com

CVE Date: October 26, 2023

Subject: CVE-2023-43208

Vulnerability Name: Mirth Connect Remote Code Execution Vulnerability

Vulnerability Type: Unauthenticated remote code execution

Information: swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures

Summary

A vulnerability exists within Mirth Connect due to its mishandling of deserialized data. This vulnerability can be leveraged by an attacker using a crafted HTTP request to execute OS commands within the context of the target application. The original vulnerability was identified by IHTeam and assigned CVE-2023-37679. 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. To exploit this vulnerability, an attacker must already be authenticated on the local network.

Affected Products

The following table lists the product impacted by the vulnerabilities listed above and the current state of remediation planning.

Product	Fix Version	Target Release Date
Pharmacy Manager	2.2.7	January 30, 2024
Delivery Manager	3.0.0	May 22, 2024

Workaround and Mitigation

Upgrade to Mirth 4.4.1 or better

In addition to the products listed above, this also affects Pharmacy Manager 1.x, Delivery Manager 2.x, PillPick and BoxPicker deployments. For these deployments, no new software release is planned. Upgrading the existing Mirth installations associated with these products to version 4.4.1 or better is the recommended mitigation.

General Security Recommendations

Swisslog Healthcare recommends upgrading to the latest SLHC software version as soon as available or upgrading to the latest Mirth software version as soon as possible.

Vulnerability Classification

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (NVD - CVSS v3 Calculator (nist.gov)). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2023-43208

To exploit this vulnerability, an unauthenticated attacker must be on the local network.

CVSS v3.1 Base Score	9.8
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE Reference	N/A

Recommended Actions

1. Swisslog Healthcare recommends upgrading to the latest SLHC or Mirth software version as soon as available.
2. Swisslog Healthcare recommends deploying the described mitigation methods until the updated software version is deployed.

Credits

None applicable.

Support and Contact Information

Product Technical Support

- Phone 24/7 support: 800-386-9666

Report a New Security Finding

- swisslog-healthcare.com/en-us/customer-care/security-information
- Product-Security@Swisslog-Healthcare.com