مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in Mirth Connect

Tracking #:432315876

Date:21-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a RCE vulnerability affecting Mirth Connect, an open-source healthcare data integration platform is actively exploited by threat actors.

TECHNICAL DETAILS:

Mirth Connect, a healthcare data integration platform, has a critical vulnerability (**CVE-2023-43208**) allowing attackers unauthorized access to potentially steal sensitive healthcare data. An earlier vulnerability (**CVE-2023-37679**) was reported and supposedly fixed in version 4.4.0.Researchers discovered the patch was incomplete, leading to CVE-2023-43208.

Affected Products: Mirth Connect versions prior to 4.4.1
Vulnerability: Unauthenticated Remote Code Execution (RCE) - **CVE-2023-43208**
Impact: Attackers can gain unauthorized access to systems, potentially leading to data exfiltration, system compromise, or ransomware deployment.
Exploitation: While a public exploit is not available, the methods for exploitation involving Java XStream are well documented, making it a high risk.
Increased Risk for Healthcare: Healthcare organizations are particularly vulnerable due to the sensitive nature of the data Mirth Connect handles. On Windows systems, where Mirth Connect commonly runs, it often operates with high privileges (SYSTEM user), further amplifying the risk.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to Upgrade Mirth Connect to version 4.4.1 or later as soon as possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://nvd.nist.gov/vuln/detail/CVE-2023-43208