مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in CData Products

Tracking #:432315821

Date:06-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed CData released security updates to fix a security vulnerability in the Jetty embedded webserver used in various products.

TECHNICAL DETAILS:

A security vulnerability has been identified that could allow a malicious actor to bypass application authentication when accessing specific endpoints that usually require authentication. This security issue applies the Java Edition CData API Server, CData Arc (ArcESB), CData Connect (On-prem), and CData Sync products and using Jetty (the default embedded Web Server).

Vulnerabilities Details:

- **CVE-2024-31848**-**Base Score: 9.8** - Path Traversal in CData API Server- A path traversal vulnerability exists in the Java version of CData API Server < 23.4.8844 when running using the embedded Jetty server, which could allow an unauthenticated remote attacker to gain complete administrative access to the application.
- **CVE-2024-31849** - **Base Score: 9.8**- Path Traversal in CData Connect- A path traversal vulnerability exists in the Java version of CData Connect < 23.4.8846 when running using the embedded Jetty server, which could allow an unauthenticated remote attacker to gain complete administrative access to the application.
- **CVE-2024-31850 - Base Score: 8.6**-Path Traversal in CData Arc- A path traversal vulnerability exists in the Java version of CData Arc < 23.4.8839 when running using the embedded Jetty server, which could allow an unauthenticated remote attacker to gain access to sensitive information and perform limited actions.
- **CVE-2024-31851 - Base Score: 8.6**-Path Traversal in CData Sync- A path traversal vulnerability exists in the Java version of CData Sync < 23.4.8843 when running using the embedded Jetty server, which could allow an unauthenticated remote attacker to gain access to sensitive information and perform limited actions.

Fixed Versions:

- CData API Server: Version: 23.4.8844+
- CData Arc (ArcESB): Version: 23.4.8839+
- CData Connect: Version: 23.4.8846+
- CData Sync: Version: 23.4.8843+

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by CData.

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://www.cdata.com/kb/entries/jetty-cve-0324.rst