Important security notification – possible vulnerability within Mitsubishi MX Component Version 3 distributed by CitectFacilities

11th April, 2013

Schneider Electric® has become aware of a public report of a heap-based buffer overflow vulnerability with proof of concept code (PoC) exploit code affecting Mitsubishi™ MX Component Version 3. This report was released without coordination with either the vendor or ICS-CERT.

The Vulnerability Identified

According to the report the vulnerability is exploitable when an attacker provides specially crafted input. The impact of this vulnerability could possibly lead to a denial of service or potentially allowing the execution of arbitrary code.

Details on Products Affected

The following Schneider Electric products distributed the Mitsubishi MX Component Version 3 trial software as a **complimentary software which was included on the DVD but not installed by default**. This trial software is not licensed by Schneider Electric and the licensed version is available from Mitsubishi.

- CitectFacilities™ v7.10 and previous versions Release Date: July 2009
- CitectSCADA™ v7.0 and previous versions Release Date: Aug 2007

The latest product versions or equivalent substitute products identified below do not provide this complimentary trial version of the software.

- CitectSCADA™ v7.20SP3 with + Facilities option
- CitectSCADA™ v7.10, v7.20, v7.30

Schneider Electric takes these reports of vulnerabilities very seriously and we have devoted resources to immediately investigate this issue.

Recommendation

Customers who may have purchased the licensed Mitsubishi MX Component Version 3 software after using the trial version should contact Mitsubishi support for possible mitigation around this vulnerability.

Additionally administrators can apply a mitigation to this vulnerability by setting the kill bit on the ActUWcd.dll ActiveX Control (CLSID B5D4B42F-AD6E-11D3-BE97-0090FE014643). See Microsoft™ KB article 240797 for additional details

We also advise any customers who may have installed Mitsubishi MX Component Version 3 trial software but are not using it, to remove it by using the uninstaller available within the “Add or remove programs” functionality.

Support

If you are unsure of whether you could be affected by this vulnerability or if you have any questions on this issue please contact the SCADA & MES Software Global Support Centre on:
http://www.citect.schneider-electric.com/contact-support

CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference, they should be adapted by individual users as required.

Base CVSS Score: 9.3 (AV:R/AC:M/Au:N/C:C/I:C/A:C)

Frequently Asked Questions

1) I am using an older release of the software discussed in this security notification. What should I do?

The affected software listed in this notification has been tested to determine which releases are affected. Other releases are past their active support life cycle.

It should be a priority for customers who have older releases of the software to migrate to supported releases to prevent potential exposure to vulnerabilities. To determine the support lifecycle for your software release, please visit the appropriate link on the product support lifecycle page on the support website accessible at

http://www.citect.schneider-electric.com/index.php?option=com_content&view=article&id=873&Itemid=632

RSS Feed

If you would like to be notified of any future security issues of interest please register for the RSS feed on our Security Notification areas:

Vijeo Citect / CitectSCADA / CitectHistorian / Vijeo Historian / Ampla / CitectFacilities Products:

> Access Controlled Proactive Notifications:
> http://www.citect.schneider-electric.com/proactive-safety-security
>
> Public Notifications:
> http://www.citect.schneider-electric.com/safety-security

Schneider Electric CyberSecurity Notifications:
http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

Version History

Version Number	Date	Comment
1.0	11th Apr 2013	Original notification released

Legal

Disclaimer

Schneider Electric is broadly distributing this Security Notification in order to bring to the attention of users of the affected products the important security information contained in this Notification. Schneider Electric recommends that all users determine the applicability of this information to their individual situations and take appropriate action. Schneider Electric does not warrant that this information is necessarily accurate or complete for all user situations and, consequently, Schneider Electric will not be responsible for any damages resulting from user's use or disregard of the information provided in this notification. To the extent permitted by law, Schneider Electric disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose, title and non-infringement.

©Copyright 2013 Schneider Electric