ICS-CERT ADVISORY

ICSA-11-279-02—CITECTSCADA AND MITSUBISHI MX4 SCADA BATCH SERVER BUFFER OVERFLOW

November 08, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-279-02P on the US-CERT secure Portal on October 06, 2011. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of Taiwan's Information and Communication Security Technology Center (ICST) has reported a buffer overflow affecting Mitsubishi MX4 Supervisory Control and Data Acquisition (SCADA). Upon further investigation, MX4 SCADA was found to be a version of CitectSCADA, a product offered by Schneider Electric. This Advisory includes a full list of known affected products.

A buffer overflow vulnerability resides in a third-party component used by the CitectSCADA and MX4 SCADA Batch products. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code.

ICS-CERT has coordinated the researcher's vulnerability report with Schneider Electric. Schneider Electric has issued a patch to address the reported vulnerability. The researcher has confirmed the patch is effective in addressing the vulnerability. Schneider Electric has provided the patch to Mitsubishi for distribution to MX4 SCADA customers.

AFFECTED PRODUCTS

The following products and versions are affected:

- CitectSCADA V7.10 and prior using the CitectSCADA Batch Server module.
- Mitsubishi MX4 SCADA V7.10 and prior using the MX4 SCADA Batch module.

IMPACT

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code on a system running an affected version of these products.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

BACKGROUND

CitectSCADA is a human-machine interface (HMI) product that is offered by Schneider Electric. MX4 SCADA is a product offered by Mitsubishi.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A buffer overflow vulnerability exists in a third-party component used by the CitectSCADA and MX4 SCADA Batch products. This vulnerability results from an overly long user input string sent to the server during the normal logon sequence. This overly long input string can allow successful exploitation of this vulnerability and can allow execution of arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill level could exploit this vulnerability.

MITIGATION

CITECTSCADA BATCH SERVER

Schneider Electric has released a notification about this vulnerability on its website, available here: http://www.citect.com/citectscada-batch.

Schneider Electric has made mitigation recommendations to customers using affected products based on their implementation and use of the Batch product.

Customers who are actively using the CitectSCADA Batch product

Schneider Electric advises these customers to contact Schneider for details on how to migrate to the new Batch platform. The BatchUninstaller is available here: http://www.citect.com/citectscada-batch-uninstaller.

Customers who run V5.50, V6.00, V6.10, V7.00, or V7.10 of CitectSCADA, but DO NOT use the Batch product

Schneider Electric recommends these customers run the CitectSCADA Batch Uninstaller to uninstall the Batch component, therefore eliminating the risk. The CitectSCADA Batch Uninstaller is available here: http://www.citect.com/citectscada-batch.

MITSUBISHI MX4 SCADA BATCH SERVER

Mitsubishi Electric Europe B.V. is contacting customers who have purchased an MX4 BATCH license and will work both with the customer and Schneider Electric to ensure they are not at risk from this vulnerability.

Mitsubishi Electric Europe B.V. has released a notification about this vulnerability on its website, available here: Mitsubishi Customer Notification

Mitsubishi recommends that customers who may have installed the MX4SCADA but are not using the MX4Batch engine (CitectSCADA Batch engine) to remove this module by using the uninstaller provided on its website:

http://www.mitsubishi-automation.com/ > Download > Product Safety NoticeAlternatively; the uninstaller can be obtained from Schneider Electric's website.

http://www.citect.com/citectscada-batch-uninstaller

Customers using MX4 Batch should contact their local Mitsubishi Electric Europe B.V. representative to discuss upgrading to a new version of the Batch platform or alternatively moving to a non-PC-based batch system such as Mitsubishi Electric Europe B.V.'s C Batch.

Mitsubishi Electric can be contacted at fa-psn@mitsubishi-automation.com for further assistance.

ADDITIONAL DEFENSIVE MEASURES

In addition to the mitigation options offered by Schneider Electric and Mitsubishi, ICS-CERT encourages asset owners to take additional defensive measures to protect against cybersecurity risks:

- ICS-CERT encourages asset owners to minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[a]

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[b] for more information on avoiding e-mail scams.
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[c] for more information on social engineering attacks.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

a. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html website last accessed November 07, 2011.

b. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed November 07, 2011.

c. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed November 07, 2011.