ICS-CERT ADVISORY

ICSA-12-102-03—MICROSYS PROMOTIC USE AFTER FREE VULNERABILITY

April 11, 2012

OVERVIEW

Independent researcher Luigi Auriemma has identified and released proof of concept code (POC) for a use after free vulnerability in the MICROSYS, spol. s r.o. PROMOTIC application without coordination with ICS-CERT, the vendor, or any other known coordinating entity.

ICS-CERT has coordinated this vulnerability with MICROSYS, which has produced an update that Mr. Auriemma confirms resolves this vulnerability.

AFFECTED PRODUCTS

The following products are affected:

- PROMOTIC versions prior to Version 8.1.7.

IMPACT

Successful exploitation of this vulnerability may result in adverse conditions ranging from the corruption of valid data to the execution of arbitrary code.

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

BACKGROUND

PROMOTIC is a Microsoft Windows based supervisory control and data acquisition human-machine interface (SCADA HMI) software programming suite for creating applications that monitor, control, and display technological processes.[a]

MICROSYS, spol. s r.o. is a Czech company with headquarters in Ostrava. The PROMOTIC system is primarily used in Czech and Slovak Republics. It is also used in Poland, Hungary, Slovenia, Serbia, Bulgaria, and Romania.

a. www.promotic.eu/, website last accessed April 11, 2012.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

USE AFTER FREE[b]

A use after free condition can occur when opening a specially crafted project file. Exploitation of this vulnerability may allow data corruption or arbitrary code execution.

CVE-2011-4874[c] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not remotely exploitable and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed project file.

EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would be difficult. Social engineering is required to convince the user to accept the malformed project file. Additional user interaction is needed to load the malformed file. This decreases the likelihood of a successful exploit.

MITIGATION

MICROSYS spol. s r.o. recommends that customers with affected versions of PROMOTIC update their installations by downloading the latest version from MICROSYS' website http://www.promotic.eu/en/firm/microsys.htm.

MICROSYS has produced a news release that contains additional information about these vulnerabilities. http://www.promotic.eu/en/pmdoc/News.htm#ver801057.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.

b. http://cwe.mitre.org/data/definitions/416.html, website last accessed April 11, 2012.
c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4874 , NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

- 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.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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*[e] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[f] 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 always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 11, 2012.
e. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed April 11, 2012.
f. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed April 11, 2012.

wish to remain anonymous. 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.