ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-333-01—MICROSYS PROMOTIC VULNERABILITY

November 29, 2011

ALERT

SUMMARY

ICS-CERT is aware of a public report of a use-after-free vulnerability with proof of concept (POC) exploit code affecting MICROSYS, spol. s r.o. PROMOTIC, a supervisory control and data acquisition (SCADA) Human-Machine Interface (HMI) product. According to this report, the vulnerability is exploitable when the program loads a specially crafted project file. This report was released by Luigi Auriemma without coordination by ICS-CERT, the vendor, or any other coordination entity that ICS-CERT is aware of.

ICS-CERT has coordinated the report with the vendor, which is working to confirm the report and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The report included vulnerability details and proof-of-concept exploit code for the following vulnerability:

Vulnerability Type	Exploitability	Impact
Use-after-free	Local	Possible Arbitrary Code Execution

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

ICS-CERT is currently reaching out to both Microsys and Computer Security Incident Response Team (CSIRT.CZ) to notify them of this vulnerability and assist them with mitigation.

BACKGROUND

MICROSYS, spol. s r.o. is a Czech company with headquarters in Ostrava. Promotic is SCADA HMI software that includes support for a web interface and is designed for Microsoft Windows.[a]

MITIGATION

ICS-CERT is currently coordinating with the vendor, security researcher, and CSIRT.CZ to identify mitigations.

[a] www.promotic.eu/, website last accessed November 29, 2011.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[b]
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ 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 System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[c]

Organizations that observe 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*[d] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[e] for more information on social engineering attacks.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ICS-CERT@DHS.GOV

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

[b] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed November 29, 2011

[c] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 29, 2011.

[d]. Recognizing and Avoiding E-mail Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed November 28, 2011.

[e]. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed November 28, 2011.

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats 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 declines attribution. 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 (ICSs) and the public at avoidable risk.