ICS-CERT ALERT

ICS-ALERT-11-286-01— MICROSYS, SPOL. S R.O. PROMOTIC MULTIPLE VULNERABILITIES

October 13, 2011

ALERT

SUMMARY

ICS-CERT is aware of a public report concerning three vulnerabilities with proof of concept (PoC) exploit code affecting MICROSYS, spol. s r.o. Promotic, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, all three vulnerabilities are remotely exploitable. This report was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has not yet verified the vulnerabilities or PoC code, but has reached out to the affected vendor to initiate a coordinated process of validation and mitigation. ICS-CERT is issuing this alert to provide early notice of the reported vulnerabilities and identify baseline mitigations for reducing risks posed by these vulnerabilities.

The report included vulnerability details and PoC exploit code for the following vulnerabilities:

Vulnerability Type	Exploitability	Impact
Directory Traversal	Remote	Data leakage
Stack Overflow	Remote	Denial of service / possible remote code execution
Heap Overflow	Remote	Denial of service / possible remote code execution

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

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 attempting to coordinate with the vendor and security researcher to identify effective mitigations.

a. www.promotic.eu/, website last accessed October 13, 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 Systems Security Program (CSSP) 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.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

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 provided when prior coordination has occurred either with 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.

b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed October 13, 2011.

c. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed October 13, 2011.