ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-024-02—MICROSYS, SPOL. S R.O. PROMOTIC MULTIPLE VULNERABILITIES

January 24, 2012

OVERVIEW

Independent researcher Luigi Auriemma has identified and released three vulnerabilities in MICROSYS, spol. s r.o. PROMOTIC application without coordination with ICS-CERT, the vendor, or any other known coordinating entity. The vulnerabilities include directory traversal, ActiveX heap overflow, and ActiveX stack overflow vulnerabilities. Public exploits are known to target these vulnerabilities.

ICS-CERT has coordinated these vulnerabilities with MICROSYS, which has produced an update. Luigi Auriemma has independently confirmed the update resolves these three vulnerabilities.

AFFECTED PRODUCTS

The following products are affected:

- PROMOTIC versions prior to Version 8.1.5.

IMPACT

Successful exploitation of these vulnerabilities may result in denial of service or data leakage.

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. This suite also includes support for a web interface.[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 January, 24, 2012.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DIRECTORY TRANSVERSAL

A directory traversal vulnerability may occur when a specially crafted request is passed to the web server running on Port 80\TCP. Successful exploitation could result in data leakage.

CVE-2011-4518[b] has been assigned to this vulnerability.

ACTIVEX STACK OVERFLOW

A stack overflow affecting an ActiveX component used by PROMOTIC may occur when a specially crafted HTML document is opened on a client machine. Successful exploitation may cause a denial of service.

CVE-2011-4519[c] has been assigned to this vulnerability.

ACTIVEX HEAP OVERFLOW

A Heap Overflow affecting an ActiveX component used by PROMOTIC may occur when a specially crafted HTML document is opened on a client machine. Successful exploitation may cause a denial of service.

CVE-2011-4520[d] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

Three of these vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level would be able to exploit these vulnerabilities.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4518, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4519, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4520, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

MITIGATION

MICROSYS recommends that customers or 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#ver80105.

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

[e] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 24, 2012.

[f] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed January 24, 2012.

[g] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed January 24, 2012.

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 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.