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

ICS-CERT ADVISORY

ICSA-12-145-01—MEASURESOFT SCADAPRO DLL HIJACK

May 24, 2012

OVERVIEW

Independent researcher Carlos Mario Penagos Hollmann identified a remotely exploitable, uncontrolled search path element vulnerability, commonly referred to as a DLL hijack, in Measuresoft’s ScadaPro application. Measuresoft has produced an upgrade to address this vulnerability. Mr. Hollmann has verified that the new version resolves the vulnerability.

AFFECTED PRODUCTS

The following Measuresoft products are affected:

- ScadaPro Server, prior to Version 4.0.0, and
- ScadaPro Client, prior to Version 4.0.0.

IMPACT

Successful exploitation of this vulnerability may lead to arbitrary code execution.

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

ScadaPro is a supervisory control and data acquisition (SCADA) system used in the power generation, oil and gas, pharmaceuticals, and manufacturing sectors. According to Measuresoft, ScadaPro is sold in multiple countries by various third-party distributors, making total deployment difficult to quantify.

Measuresoft Development Ltd. is headquartered in Louth, Ireland, with an office in Missouri City, Texas.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

UNCONTROLLED SEARCH PATH ELEMENT[a]

ScadaPro uses a fixed or controlled search path to find resources, which could allow an unauthorized user to easily locate and exploit one or more locations. An unauthorized user could place a malicious DLL in a directory where it could be loaded before the valid DLL. An attacker must have access to the host file system to exploit this vulnerability. If exploited, this vulnerability could allow execution of arbitrary code.

CVE-2012-1824[b] has been assigned to this vulnerability. A CVSS v2 base score of 6 has been assigned; the CVSS vector string is (AV:L/AC:H/Au:S/C:C/I:C/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be remotely exploited.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a moderate skill level could be able to exploit these vulnerabilities.

MITIGATION

Measuresoft has produced an upgrade to address this vulnerability. Links to the upgrade can be found here:

- ScadaPro Server: http://www.measuresoft.net/download/versions.aspx?v=CB&d=Server, and
- ScadaPro Client: http://www.measuresoft.net/download/versions.aspx?v=CB&d=Client.

Microsoft has also released a Security Advisory (2269637).[d]

[a] CWE, http://cwe.mitre.org/data/definitions/427.html, Web site last accessed May 25, 2012.

[b] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1824, NIST uses this ICS-CERT Advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[c] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:H/Au:S/C:C/I:C/A:C), Web site last visited May 25, 2012.

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

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams[e] for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks[f] for more information on social engineering attacks.
- 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.[g] 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.

[d] Microsoft Security Advisory, http://technet.microsoft.com/en-us/security/advisory/2269637, Web site visited May 25, 2012.

[e] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed May 25, 2012

[f] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed May 25, 2012

[g] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed May 25, 2012.

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

ICS-CERT CONTACT

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

Email: 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.