ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-263-01—MEASURESOFT SCADAPRO MULTIPLE VULNERABILITIES

September 20, 2011

OVERVIEW

This Advisory is a follow-up to the Alert titled "ICS-ALERT-11-256-04—Measuresoft ScadaPro" that was published September 13, 2011, on the ICS-CERT website.

ICS-CERT is aware of a public report of three vulnerabilities with proof-of-concept (PoC) exploit code affecting Measuresoft ScadaPro. According to the report, the vulnerabilities include a stack buffer overflow, an insecure method call, and a path traversal, which are all remotely exploitable through Port 11234/UDP. This report was released publicly without coordination with either the vendor or ICS-CERT.

Attribution for the discovery of these vulnerabilities is not provided in this advisory because no prior coordination occurred with the vendor, ICS-CERT, or other coordinating body. 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.

ICS-CERT has coordinated with Measuresoft, which has produced a fix that resolves these vulnerabilities. The fix has been tested to validate that it resolves the vulnerabilities.

AFFECTED PRODUCTS

The following Measuresoft ScadaPro versions are affected:

- ScadaPro Version 4.0.0.0 and earlier.

IMPACT

The stack overflow vulnerability could allow an attacker to cause a denial of service (DoS) or to remotely execute code on the affected machine. The insecure method call and the path traversal vulnerabilities could allow information 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 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

Vulnerability Type	Exploitability	Impact
Stack Overflow	Remote	Denial of Service / Possible Remote Code Execution
Insecure Method Call	Remote	Information Leak / Disclosure
Path Traversal	Remote	Information Leak / Disclosure

MITRE[a] has assigned numbers CVE-2011-3490, CVE-2011-3495, CVE-2011-3496, and CVE-2011-3497 to these vulnerabilities in the Common Vulnerabilities and Exposures database.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to exist that target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level can create a DoS, traverse directories, or extract data; only a more skilled attacker would be able to execute arbitrary code on affected systems.

[a] http://cve.mitre.org/cve/, website last accessed September 20, 2011.

MITIGATION

Measuresoft has provided a new version (4.0.1), which is available without cost to all licensed customers who are currently running Version 4.0.0. Measuresoft has resolved the reported issues by disabling Port 11234/UDP by default. According to Measuresoft, alternative network communication methods are already in place and will be used instead.

According to Measuresoft, Version 4.0.1 of ScadaPro Server is now available for download from the Measuresoft website: http://www.measuresoft.com/download/current_release.aspx.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks. Asset owners should consider the following measures:

- 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.

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 section for control system 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.*[b]

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* [c] for more information on avoiding e-mail scams

[b] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 20, 2011.

[c] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed September 20, 2011.

3. Refer to *Avoiding Social Engineering and Phishing Attacks*[d] 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.

[d] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed September 20, 2011.