



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

# ICS-CERT ALERT

ICS-ALERT-11-256-04—MEASURESOF SCADAPRO MULTIPLE VULNERABILITIES

September 13, 2011

## ALERT

### SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (POC) exploit code affecting Measuresoft ScadaPro. According to the report, the vulnerabilities are remotely exploitable through Port 11234/UDP. This report was released without coordination with the vendor or with ICS-CERT.

ICS-CERT has not yet verified the vulnerabilities or POC code, but has reached out to the affected vendor to notify, confirm, 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.

Initial analysis of the report indicates vulnerability details and proof-of-concept exploit code for the following vulnerabilities:

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

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

### BACKGROUND

ScadaPro is a supervisory control and data acquisition (SCADA) system used in power generation, oil and gas, pharmaceuticals, and manufacturing. Measuresoft Development Ltd. is headquartered in Louth, Ireland with an office in Missouri City, Texas.

### MITIGATION

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



## ICS-CERT

### INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.<sup>a</sup>
- 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).

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*.<sup>b</sup>

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](mailto:ICS-CERT@DHS.GOV)

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

---

a. ICS-CERT ALERT, [http://www.us-cert.gov/control\\_systems/pdf/ICS-Alert-10-301-01.pdf](http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf), accessed September 13, 2011.

b. Control System Security Program (CSSP) Recommended Practices, [http://www.us-cert.gov/control\\_systems/practices/Recommended\\_Practices.html](http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html), accessed September 13, 2011.