ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

# ICS-CERT ADVISORY

## ICSA-12-249-03—INDUSOFT ISSYMBOL ACTIVEX CONTROL BUFFER OVERFLOW

September 05, 2012

## OVERVIEW

ICS-CERT received a report from Indusoft and the Zero Day Initiative (ZDI)[a] concerning a heap-based buffer overflow vulnerability affecting the InduSoft ISSymbol ActiveX control. This vulnerability was reported to ZDI by security researcher Alexander Gavrun.

Successful exploitation of this vulnerability could allow remote execution of arbitrary code.

## AFFECTED PRODUCTS

The following products and versions are affected:

- InduSoft ISSymbol ActiveX Control (Build 301.1009.2904.0),
- InduSoft Thin Client Version 7.0, and
- InduSoft Web Studio Version 7.0B2

## IMPACT

Successful exploitation of the reported vulnerability could allow an attacker to perform arbitrary code execution. These actions can result in adverse application conditions and ultimately impact the production environment on which the supervisory control and data acquisition (SCADA) system is used.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

## BACKGROUND

InduSoft Web Studio is a collection of automation tools to develop human-machine interfaces, SCADA systems, and embedded instrumentation systems. InduSoft products are often integrated as third-party components in other vendors’ products.

[a] http://www.zerodayinitiative.com/, Web site last accessed September 05, 2012.

# VULNERABILITY CHARACTERIZATION

## VULNERABILITY OVERVIEW

### HEAP-BASED BUFFER OVERFLOW[b]

Boundary errors on processing the “InternationalOrder” and “InternationalSeparator” properties can be exploited causing a heap-based buffer overflow via an overly long string assigned to the properties.

CVE-2011-0340[c] has been assigned to this vulnerability. According to ZDI, a CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).[d]

## VULNERABILITY DETAILS

### EXPLOITABILITY

This vulnerability could be exploited remotely.

### EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

### DIFFICULTY

This vulnerability requires moderate skills to exploit.

# MITIGATION

ICS-CERT recommends that customers of InduSoft Web Studio software take the following mitigation steps.

- Apply hotfix 70.1.02.12. The InduSoft security patch and details are available at: http://www.indusoft.com/hotfixes/hotfixes.php.
- NOTE: Users will be required to email InduSoft support to acquire the hotfix. The link on the InduSoft Web site will automatically draft an email to Support with a request.

[b] CWE, http://cwe.mitre.org/data/definitions/122.html, CWE-122: Heap-based Buffer Overflow, Web site last accessed September 05, 2012.

[c] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0340 , Web site last accessed September 05, 2012.

[d] NVD, http://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=%28AV:N/AC:L/Au:N/C:P/I:P/A:P%29 , Web site last accessed September 05, 2012.

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.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[f] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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.

## 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

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

[e] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 05, 2012.

[f] Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 05, 2012.

## 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.