ICS-CERT ADVISORY

ICSA-11-273-02—INDUSOFT ISSYMBOL ACTIVEX CONTROL BUFFER OVERFLOW

September 30, 2011

OVERVIEW

ICS-CERT has received a report from independent security researcher Dmitriy Pletnev of Secunia Research[a] about ActiveX control buffer overflow vulnerabilities with proof-of-concept exploit code affecting the InduSoft ISSymbol product. Secunia has coordinated with InduSoft, who has produced a patch that mitigates these vulnerabilities. ICS-CERT has not validated the patch.

AFFECTED PRODUCTS

The vulnerabilities affect InduSoft Web Studio Versions 7.0B2 (Build: 0301.1009.2904.0000) and 7.0 (Build: 0301.1102.0303.0000).

IMPACT

An attacker who successfully exploits any of these vulnerabilities may be able to execute arbitrary code on the target system.

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

InduSoft Web Studio is used to develop human-machine interfaces, SCADA systems, and embedded instrumentation systems. InduSoft is often integrated as a third-party application in control systems.

a. http://secunia.com/secunia_research/2011-61/, website last visited September 30, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Boundary errors on processing the "Open," "Close," and "SetCurrentLanguage" methods for this ActiveX control can be exploited to cause heap and stack-based buffer overflows via overly long strings assigned to the properties.

CVE-2011-0342 has been assigned for these vulnerabilities.[b] A CVSS base score of 10.0 has been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level can create the denial of service; an attacker would require more skill to execute arbitrary code.

MITIGATION

InduSoft recommends that customers of InduSoft Web Studio software upgrade to the latest version and install the latest service pack. The latest service pack is available for download at InduSoft's Security Updates and Hotfixes webpage at http://www.indusoft.com/hotfixes/hotfixes.php.

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.

b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0342, website last accessed September 30, 2011.

- 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 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.*[c] 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.

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.

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 30, 2011.