ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-168-01—INDUSOFT ISSYMBOL ACTIVEX CONTROL BUFFER OVERFLOWS

June 17, 2011

OVERVIEW

Security researcher Dmitriy Pletnevo of Secunia Research[a] has released details of multiple overflow vulnerabilities affecting the InduSoft ISSymbol ActiveX control. The researcher identified both stack-based and heap-based buffer overflows.

Successful exploitation of these vulnerabilities allows execution of arbitrary code.

ICS-CERT has confirmed that Secunia and InduSoft coordinated this vulnerability prior to public release of this report. InduSoft has issued an update addressing this vulnerability. Secunia has validated that the patch addresses the arbitrary code execution.

AFFECTED PRODUCTS

The researcher reports that the zero-day vulnerability affects the following InduSoft Products:

- InduSoft ISSymbol ActiveX Control (build 301.1009.2904.0)
- InduSoft Thin Client Version 7.0
- InduSoft Web Studio Version 7.0B2.

IMPACT

Successful exploitation of the reported vulnerabilities can 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 that provide building blocks to develop human-machine interfaces, SCADA systems, and embedded instrumentation solutions. InduSoft is often integrated as a third-party application in control systems.

[a] Secunia Research, http://secunia.com/secunia_research/2011-36/, website last accessed June 16, 2011.

VULNERABILITY CHARACTERIZATION

HEAP-BASED BUFFER OVERFLOW VULNERABILITY OVERVIEW

Boundary errors on processing the "InternationalOrder" and "InternationalSeparator" properties can be exploited to cause a heap-based[b] buffer overflow via an overly long string assigned to the properties.

HEAP-BASED BUFFER OVERFLOW VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable by sending specially crafted code to the InduSoft Web server.

EXISTENCE OF EXPLOIT

No exploits are known specifically to target this vulnerability.

DIFFICULTY

This vulnerability requires moderate skills to exploit.

STACK-BASED BUFFER OVERFLOW VULNERABILITY OVERVIEW

The researcher reports,[c] "A boundary error when processing a certain window procedure can be exploited to cause a stack-based buffer overflow[d] via e.g., an overly long string passed as the 'bstrFileName' parameter to the 'OpenScreen()' method.

"A boundary error when creating a log file can be exploited to cause a stack-based buffer overflow via an overly long string assigned to the 'LogFileName' property."

STACK-BASED BUFFER OVERFLOW VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable by sending specially crafted code to the InduSoft Web server.

EXISTENCE OF EXPLOIT

No exploits are known specifically to target this vulnerability.

DIFFICULTY

This vulnerability requires moderate skills to exploit.

[b] MITRE, http://cwe.mitre.org/data/definitions/122.html, website last accessed June 16, 2011.

[c] Secunia Research, http://secunia.com/secunia_research/2011-36/, website last accessed June 16, 2011.

[d] MITRE, http://cwe.mitre.org/data/definitions/121.html, website last accessed June 16, 2011.

MITIGATION

VENDORS INCORPORATING INDUSOFT WEB STUDIO

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

- Upgrade to the latest version and install the latest patch. The InduSoft security patch is available for download at: http://www.indusoft.com/hotfixes/hotfixes.php

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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT encourages asset owners to minimize network exposure for all control systems devices. Critical devices should not directly face the Internet. Locate control systems 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).

The Control Systems Security Program (CSSP) also provides a section for control system security recommended practices on the CSSP page of the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[e]

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.

[e] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed June 16, 2011.