ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-319-01—INDUSOFT WEB STUDIO MULTIPLE REMOTE VULNERABILITIES

November 15, 2011

OVERVIEW

ICS-CERT has become aware of a report from the Zero Day Initiative concerning two vulnerabilities in the InduSoft Web Studio software. This information was reported to Zero Day Initiative by independent security researcher Luigi Auriemma.

These vulnerabilities exploit unauthenticated remote code execution within the CEServer Operation and the CEServer.exe directories.

Zero Day Initiative has coordinated with InduSoft, who has produced a patch that mitigates these vulnerabilities.

AFFECTED PRODUCTS

According to InduSoft, these vulnerabilities affect the following products:

InduSoft Web Studio Versions 6.1 and 7.0.

IMPACT

An attacker who successfully exploits these vulnerabilities can execute arbitrary code on the targeted 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 operational environment, architecture, and product implementation.

BACKGROUND

According to InduSoft, Web Studio is a collection of automation tools used to develop human-machine interfaces, supervisory control and data acquisition (SCADA) systems, and embedded instrumentation solutions. Web Studio is a software product sold worldwide in industries dealing with system automation.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

UNAUTHENTICATED REMOTE CODE EXECUTION

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of InduSoft Web Studio. The vulnerability exists within the remote agent component (CEServer.exe) that listens by default on Port 4322/TCP. When handling incoming requests, the process fails to perform any type of authentication.

CVE-2011-4051[a] has been assigned to this vulnerability.

REMOTE CODE EXECUTION

This vulnerability allows unauthenticated remote attackers to execute arbitrary code on vulnerable installations of InduSoft Web Studio. This vulnerability exists within the CEServer component, which is used as a runtime dependency for deployed applications that use InduSoft Web Studio. When handling the remove file operation (0x15), the process blindly copies user-supplied data to a fixed-length buffer on the stack.

CVE-2011-4052[b] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits exist that target these vulnerabilities.

DIFFICULTY

An attacker with a moderate skill level could exploit these vulnerabilities.

[a] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4051. This website will be active sometime after publication of this advisory.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4052. This website will be active sometime after publication of this advisory.

MITIGATION

InduSoft recommends that customers of InduSoft Web Studio software 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.

In addition to installing the latest version and patch of InduSoft Web Studio, 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.*[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 November 14, 2011.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. 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.