ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-006-01—3S SMART SOFTWARE SOLUTIONS CODESYS VULNERABILITIES

January 06, 2012

OVERVIEW

Security researcher Celil Unuver (SignalSec LLC[a]) and independent researcher Luigi Auriemma have identified multiple vulnerabilities in the 3S Smart Software Solutions CoDeSys product, summarized in the following table. Mr. Auriemma publicly disclosed the five vulnerabilities along with proof-of-concept (PoC) exploit code, including the vulnerability previously coordinated with ICS-CERT by Celil Unuver, without coordination with 3S Smart Software Solutions, ICS-CERT, or any other coordinating entity known to ICS-CERT.

ICS-CERT has coordinated these vulnerabilities with 3S Smart Software Solutions, and they have produced new versions for both CoDeSys V3 and V2.3 that mitigate these vulnerabilities. Mr. Auriemma has confirmed that the new versions fully resolve the reported vulnerabilities.

Researcher	Vulnerability	Coordinated/Unanticipated	CVE
Luigi Auriemma	Integer Overflow	Unanticipated	CVE-2011-5008
Luigi Auriemma Celil Unuver	Stack Overflow	Unanticipated Coordinated	CVE-2011-5007
Luigi Auriemma	Content-Length NULL Pointer	Unanticipated	CVE-2011-5009
Luigi Auriemma	Invalid HTTP Request NULL Pointer	Unanticipated	CVE-2011-5009
Luigi Auriemma	Folders Creation	Unanticipated	None

AFFECTED PRODUCTS

The following 3S Smart Software Solutions CoDeSys versions are affected:

- Version 2.3
- Version 3.4.

[a] SignalSEC LLC, www.signalsec.com website last accessed January 06, 2012.

IMPACT

Successful exploitation of these vulnerabilities may allow an attacker to cause a denial of service (DoS) or to execute arbitrary code.

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

CoDeSys is produced by 3S Smart Software Solutions GmgH based in Germany.

According to the 3S Smart Software Solutions website,[b] CoDeSys is used across several sectors of the automation industry by manufacturers of industrial controllers or intelligent automation devices and by end users in different industries including system integrators who offer automation solutions using CoDeSys.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INTEGER OVERFLOW

An attacker could exploit this vulnerability by sending specially crafted packets to Port 1217/TCP.

CVE-2011-5008[c] has been assigned to this vulnerability.

STACK OVERFLOW

An attacker could exploit this vulnerability by sending an overly long URL to Port 8080/TCP.

CVE-2011-5007[d] has been assigned to this vulnerability.

CONTENT-LENGTH NULL POINTER

An attacker could exploit this vulnerability by sending a specially crafted Content-Length header to Port 8080/TCP.

CVE-2011-5009[e] has been assigned to this vulnerability.

[b] http://www.3s-software.com website last accessed January 06, 2012.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5008, website last accessed January 06, 2012.

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5007, website last accessed January 06, 2012.

[e] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5009, website last accessed January 06, 2012.

INVALID HTTP REQUEST NULL POINTER

An attacker could exploit this vulnerability by sending a request with an unknown HTTP method to Port 8080/TCP.

CVE-2011-5009[f] has been assigned to this vulnerability.

FOLDERS CREATION

An attacker could exploit this vulnerability by sending a web request containing a nonexistent directory to Port 8080/TCP. Exploitation of this vulnerability results in the creation of arbitrary directories.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

DIFFICULTY

An attacker with a low skill level can create the DoS, whereas it would require a more skilled attacker to execute arbitrary code.

MITIGATION

3S Smart Software Solutions has developed a new version of CoDeSys that resolves these vulnerabilities (V3.5 and V2.3.9.32). Customers can download the new versions for CoDeSys from the 3S Smart Software Solutions customer download website located at:

http://www.3s-software.com/index.shtml?en_download.

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.

[f] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5009, website last accessed January 06, 2012.

- 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.*[g] 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.

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.

[g] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 06, 2012.