ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-011-01—3S CODESYS MULTIPLE VULNERABILTIES

January 11, 2013

OVERVIEW

This advisory is a follow-up to the ICS-CERT Alert titled "ICS-ALERT-12-097-02A—3S-Software CoDeSys Improper Access Control (Update)" that was published October 26, 2012, on the ICS-CERT Web page.[a] This advisory provides mitigation details for multiple vulnerabilities that affect the 3S-Smart Software Solutions CoDeSys Runtime Toolkit.

Independent researcher Reid Wightman of IOActive, formerly of Digital Bond, identified[b] an improper access control and a directory traversal vulnerability in the 3S CoDeSys Runtime application without coordination with ICS-CERT, the vendor, or any other coordinating entity known to ICS-CERT. Exploitation of these vulnerabilities would allow unauthorized access to the system and unauthorized access to the file system. The CoDeSys Runtime Toolkit is used in a number of vendor's products worldwide. 3S has developed a patch that implements a password for authentication to the system. Reid Wightman has validated that the patch, issued by 3S, mitigates theses vulnerabilities.

These vulnerabilities can be exploited remotely. Exploits that target these vulnerabilities are known to be publicly available. This researcher has released proof-of-concept (PoC) code for these vulnerabilities.

AFFECTED PRODUCTS

The following 3S CoDeSys Runtime versions are affected:

- CoDeSys Version 2.3.X
- CoDeSys Version 2.4.X

Note: CoDeSys Version 3.X is not affected by these vulnerabilities.

a. ICS-ALERT-12-097-02A—3S-Software CoDeSys Improper Access Control (Update), http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-097-02A.pdf, Web page last accessed January 11, 2013.
b. 3S CoDeSys Disclosure, http://www.digitalbond.com/tools/basecamp/3s-codesys/, Web page last accessed January 11, 2013.

IMPACT

The improper access control vulnerability allows attackers to gain unauthorized administrative access to the device. Once access is obtained, the attacker has the ability to perform privileged operations without a password. Attackers can also exploit the directory traversal vulnerability to read and write to the file system.

The 3S CoDeSys Runtime Toolkit is an embedded system that is used in a wide variety of different products manufactured by various vendors. 3S published a list of devices on their Web page that contained their products, but this has since been removed. It is believed that the CoDeSys Runtime Toolkit is used in over 260 individual products.

Devices and programmable logic controllers (PLCs) that use the embedded CoDeSys Runtime Toolkit are used in various industries to include critical manufacturing, energy, transportation, and others. Devices containing CoDeSys are impacted.

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

3S-Smart Software Solutions is a German-based company that maintains offices in Germany and China. 3S develops software that is used in various PLC and industrial controllers. 3S also develops products specifically for visualization applications (HMIs), engineering desktop programming platforms, safety modules, and fieldbus controllers.

The affected product, CoDeSys Runtime Toolkit, is embedded third-party software used in various manufacturers' SCADA systems. According to 3S, CoDeSys is deployed across several sectors including critical manufacturing, building automation, energy, transportation, and others. 3S estimates that these products are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER ACCESS CONTROL[c]

The CoDeSys Runtime Toolkit does not require users to authenticate when connecting to the device. An attacker could obtain administrative privileges on the device by default. This could allow the attacker to compromise the availability, integrity, and confidentiality of the device.

CVE-2012-6068[d] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[e]

DIRECTORY TRAVERSAL[f]

The CoDeSys Runtime Toolkit's file transfer functionality does not perform input validation, which allows an attacker to access files and directories outside the intended scope. This allows an attacker to upload and download any file on the device. This could allow the attacker to affect the availability, integrity, and confidentiality of the device.

CVE-2012-6069[g] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[h]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

c. Improper Authentication, http://cwe.mitre.org/data/definitions/284.html, CWE-284: Improper Access Control, Web site last accessed January 11, 2013.

d. NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-6068 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C), Web site last visited January 11, 2013.

f. Relative Path Traversal, http://cwe mitre.org/data/definitions/23 html, CWE-23: Relative Path Traversal, Web site last accessed January 11, 2013.

g. NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-6069 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

h. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C), Web site last visited January 11, 2013.

EXISTENCE OF EXPLOIT

Exploits that target these vulnerabilities are publicly available.

DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities.

MITIGATION

3S released a press release concerning these vulnerabilities to their News & Events page,[i] which details the patch released to mitigate the vulnerabilities. The patch released by 3S implements a password for authentication to the device. The patch can be downloaded from the CoDeSys Download Center.[j] 3S also recommends the usage of standard security methods like firewalls or Virtual Private Network (VPN) access to prevent unauthorized access to the controller.

CoDeSys version 3.X is not affected by these vulnerabilities.

ICS-CERT encourages asset owners to upgrade to version 3 and 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 VPNs, recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[k] 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—Targeted Cyber Intrusion

i. 3S Press Release, http://www.codesys.com/news-events/press-releases/detail/article/sicherheitsluecke-in-codesys-v23-laufzeitsystem.html, Web page last accessed January 11, 2013.

j. CoDeSys Download Center, http://www.codesys.com/download html, Web site last accessed January 11, 2013.

k. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 11, 2013.

Detection and Mitigation Strategies,[l] 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@hq.dhs.gov
Toll Free: 1-877-776-7585

For industrial control systems security 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/.

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.

l. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed January 11, 2013.