ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-016-01—SCHNEIDER ELECTRIC AUTHENTICATED COMMUNICATION RISK VULNERABILITY

January 16, 2013

OVERVIEW

ICS-CERT has received a report from Schneider Electric concerning an Authenticated Communication Risk vulnerability in the Schneider Electric Software Update utility (SESU). This vulnerability was reported to Schneider Electric by security researcher Arthur Gervais.

The SESU is a centralized update mechanism for updating Schneider Electric software on Windows PC. Schneider Electric has updated the SESU client as of January 2013, which adds the use of HTTPS to resolve this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

According to Schneider Electric, the following products and versions are affected by use of the SESU mechanism:

- Unity Pro, V5.0 L, M, S, XL,
- Unity Pro, V6.0 L, M, S, XL,
- Unity Pro, V6.1 L, M, S, XL,
- Unity Pro, V0 L, M, S, XL, XLS,
- Vijeo Designer V6.0.x, V6.1.0.x, V5.0.0.x, V5.1.0.x,
- Vijeo Designer Opti V6.0.x, V5.1.0.x, V5.0.0.x,
- Web Gate Client Files V5.1.x,
- IDS V1.0, V2.0,
- PowerSuite 2.5,
- Smart Widget Acti 9 V1.0.0.0,

- Smart Widget H8035 V1.0.0.0,
- Smart Widget H8036 V1.0.0.0,
- Smart Widget PM201 V1.0.0.0,
- Smart Widget PM710 V1.0.0.0,
- Smart Widget PM750 V1.0.0.0,
- SoMachine V1.2.1,
- Spacail.pro V1.0.0.x, and
- SESU V1.0.x, V1.1.x

IMPACT

Successfully exploiting this vulnerability could result in arbitrary code execution.

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 operational environment, architecture, and product implementation.

BACKGROUND

Schneider Electric is a manufacturer and integrator of energy management equipment and software. According to Schneider Electric, their products are used in energy, industry, and building automation worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

AUTHENTICATED COMMUNICATIONS RISK[a]

Schneider Electric software on the customer PC uses the SESU service as the mechanism of communication with the Schneider Electric central update server in order to receive periodic software updates. The SESU client on the customer PC does not check the authenticity of the origin. By redirecting messages to Port 80/TCP on an unauthorized source, an attacker could execute arbitrary code on a vulnerable system that could result in loss of availability, integrity, and confidentiality.

a. CWE-287: Improper Authentication, http://cwe.mitre.org/data/definitions/287.html, CWE-287, Improper Authentication, Web site last accessed January 16, 2013.

CVE-2013-0655[b] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits exist that target this vulnerability.

DIFFICULTY

An attacker with a medium skill level would be able to exploit this vulnerability.

MITIGATION

Schneider Electric has produced a customer notification[d] that contains mitigations to resolve this vulnerability. According to Schneider Electric, in order to resolve the vulnerability with the software server, Schneider Electric has taken the following actions:

1. The SESU server has been updated to the latest version. Currently, both HTTP and HTTPS are supported in parallel. HTTPS does ensure signed communication.
2. The new SESU client has been updated as of January 2013 to use HTTPS instead of HTTP. The new version of the SESU Client will be made available to customers for distribution via the SESU mechanism in January 2013.
3. Customers can also use an updated software product CD that will contain the updated SESU client, when the CD becomes available. Contact your local support desk for details.
4. While both HTTP and HTTPS SESU client functionality is supported currently, several months after starting to update the SESU clients (May 2013) the HTTP port of the SESU

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0655, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last accessed January 16, 2013.
d. Schneider Electric Customer Notification, http://www2.schneider-electric.com/corporate/en/support/cybersecurity/viewer-news.page?c_filepath=/templatedata/Content/News/data/en/local/cybersecurity/general_information/2013/01/20130109_advisory_of_vulnerability_affecting_schneider_electric_s_software_upda.xml, Web site last accessed January 16, 2012.

server will be disabled. This means that only HTTPS will be supported during SESU client updates from that time forward, which mitigates this current vulnerability.

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.

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.[e] 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 Detection and Mitigation Strategies,[f] 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

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 16, 2013.

f. 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 16, 2013.

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.