



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

# ICS-CERT ADVISORY

## ICSA-12-325-01—SINAPSI DEVICES MULTIPLE VULNERABILITIES

November 20, 2012

### OVERVIEW

This advisory is a follow-up to the alert titled ICS-ALERT-12-284-01—Sinapsi eSolar Light Multiple Vulnerabilities that was published October 10, 2012, on the ICS-CERT Web page.<sup>a</sup>

Independent researchers Roberto Paleari and Ivan Speziale identified four vulnerabilities and released proof-of-concept (exploit) code for the Sinapsi eSolar Light Photovoltaic System Monitor without coordination with ICS-CERT, this vendor, or any other coordinating entity known to ICS-CERT.

The eSolar Light has also been sold with different brands and names. Successful exploitation of the vulnerabilities would allow an attacker to gain unauthorized access, access private information, and execute remote code. The eSolar Light is a monitoring system used in solar power applications. However, Sinapsi also reports that other Sinapsi devices (eSolar, eSolar DUO, eSolar Light) are vulnerable to these vulnerabilities. These devices are used in the Energy Sector.

### AFFECTED PRODUCTS

The following Sinapsi devices with firmware prior to Version 2.0.2870\_xxx\_2.2.12 are affected:

- eSolar,
- eSolar DUO, and,
- eSolar Light.

a. ICS-ALERT-12-284-01—Sinapsi eSolar Light Photovoltaic System Monitor Multiple Vulnerabilities, [http://www.us-cert.gov/control\\_systems/pdf/ICS-ALERT-12-284-01.pdf](http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-284-01.pdf), Web site last visited November 20, 2012.

This product is provided subject only to the Notification Section as indicated here: <http://www.us-cert.gov/privacy/>



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

### IMPACT

Malicious attackers could use the vulnerabilities to exploit the device by gaining unauthorized access in the system, leaking stored information, and remotely executing code on the device. This could allow a loss of availability, integrity, and confidentiality of the affected system. Because Sinapsi devices are primarily used for control and monitoring of energy systems, the Energy Sector is affected. Some Sinapsi devices are also used for building automation.

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

Sinapsi is an Italian-based company that sells devices used for energy monitoring and management as well as building automation applications.

The affected products are Web-based SCADA monitoring and management systems. According to Sinapsi, the products are deployed across the Energy Sector and also used for building automation. Sinapsi estimates that these products are used primarily in Italy, but some vendors have marketed the products in the United States and other countries.

## VULNERABILITY CHARACTERIZATION

### VULNERABILITY OVERVIEW

#### **HARD-CODED CREDENTIALS<sup>b</sup>**

The Sinapsi devices store hard-coded passwords in the PHP file of the device. By using the hard-coded passwords in the device, attackers can log into the device with administrative privileges. This could allow the attacker to have unauthorized access.

CVE-2012-5862<sup>c</sup> 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).<sup>d</sup>

b. CWE, <http://cwe.mitre.org/data/definitions/259.html>, CWE-259: Hard-Coded Password, Web site last accessed November 20, 2012.

c. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5862>, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

d. CVSS Calculator, [http://nvd.nist.gov/cvss.cfm?version=2&vector=\(AV:N/AC:L/Au:N/C:C/I:C/A:C\)](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 November 20, 2012.



## ICS-CERT

### INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

---

#### SQL INJECTION<sup>e</sup>

The Sinapsi devices do not check the validity of the data before executing queries. By accessing the SQL table of certain pages that do not require authentication within the device, attackers can leak information from the device. This could allow the attacker to compromise confidentiality.

CVE-2012-5861<sup>f</sup> has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:N/A:N).<sup>g</sup>

---

#### OPERATING SYSTEM COMMAND INJECTION<sup>h</sup>

The Sinapsi devices do not check for special elements in commands sent to the system. By accessing certain pages with administrative privileges that do not require authentication within the device, attackers can execute arbitrary, unexpected, or dangerous commands directly onto the operating system.

CVE-2012-5863<sup>i</sup> 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).<sup>j</sup>

---

#### BROKEN SESSION ENFORCEMENT<sup>k</sup>

The Sinapsi devices do not check if users that visit pages within the device have properly authenticated. By directly visiting the pages within the device, attackers can gain unauthorized access with administrative privileges.

---

e. CWE, <http://cwe.mitre.org/data/definitions/89.html>, CWE-89: SQL Injection, Web site last accessed November 20, 2012.

f. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5861>, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

g. CVSS Calculator, [http://nvd.nist.gov/cvss.cfm?version=2&vector=\(AV:N/AC:L/Au:N/C:C/I:N/A:N\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:N/A:N)), Web site last visited November 20, 2012.

h. CWE, <http://cwe.mitre.org/data/definitions/78.html>, CWE-78: OS Command Injection, Web site last accessed November 20, 2012.

i. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5863>, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

j. CVSS Calculator, [http://nvd.nist.gov/cvss.cfm?version=2&vector=\(AV:N/AC:L/Au:N/C:C/I:C/A:C\)](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 November 20, 2012.

k. CWE, <http://cwe.mitre.org/data/definitions/287.html>, CWE-287: Improper Authentication, Web site last accessed November 20, 2012.



## ICS-CERT

### INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CVE-2012-5864<sup>l</sup> has been assigned to this vulnerability. A CVSS v2 base score of 9.4 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:N).<sup>m</sup>

#### VULNERABILITY DETAILS

##### EXPLOITABILITY

These vulnerabilities could be exploited remotely.

##### 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

Sinapsi has developed a new firmware version 2.0.2870\_2.2.12 that mitigates these vulnerabilities. Sinapsi released the new firmware on Monday, November 19, 2012 directly to the devices. Users will be able to manually download the firmware on their device by using the Firmware Update function in the System Menu in the device's Web interface. Sinapsi has also posted a security newsletter to its public Web site.<sup>n</sup>

Other affected vendors have been notified by Sinapsi and ICS-CERT, but the availability of new firmware upgrades are unknown by ICS-CERT at this time.

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.

---

l. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5864>, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

m. CVSS Calculator, [http://nvd.nist.gov/cvss.cfm?version=2&vector=\(AV:N/AC:L/Au:N/C:C/I:C/A:N\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:N)), Web site last visited November 20, 2012.

n. Sinapsi Security Pack New Release (Italian), [http://www.sinapsitech.it/default.asp?active\\_page\\_id=78&news\\_id=88](http://www.sinapsitech.it/default.asp?active_page_id=78&news_id=88), Web site last visited November 20, 2012.



## ICS-CERT

### INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- 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.<sup>o</sup> 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—Cyber Intrusion Mitigation Strategies,<sup>p</sup> that is available for download from the ICS-CERT Web page ([www.ics-cert.org](http://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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click Web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams<sup>q</sup> for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks<sup>r</sup> for more information on social engineering attacks.

## ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: [ics-cert@dhs.gov](mailto:ics-cert@dhs.gov)

Toll Free: 1-877-776-7585

For industrial control systems security information and incident reporting: [www.ics-cert.org](http://www.ics-cert.org)

---

o. CSSP Recommended Practices, [http://www.us-cert.gov/control\\_systems/practices/Recommended\\_Practices.html](http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html), Web site last accessed November 20, 2012.

p. Cyber Intrusion Mitigation Strategies, [http://www.us-cert.gov/control\\_systems/pdf/ICS-TIP-12-146-01A.pdf](http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf), Web site last accessed November 20, 2012.

q. Recognizing and Avoiding Email Scams, [http://www.us-cert.gov/reading\\_room/emailscams\\_0905.pdf](http://www.us-cert.gov/reading_room/emailscams_0905.pdf), Web site last accessed November 20, 2012.

r. National Cyber Alert System Cyber Security Tip ST04-014, <http://www.us-cert.gov/cas/tips/ST04-014.html>, Web site last accessed November 20, 2012.



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

---

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.