ICS-CERT ADVISORY

ICSA-13-018-01—SCHNEIDER ELECTRIC IGSS BUFFER OVERFLOW

January 18, 2013

OVERVIEW

Independent researcher Aaron Portnoy of Exodus Intelligence has identified a buffer overflow vulnerability in Schneider Electric's Interactive Graphical SCADA System (IGSS) application. Schneider Electric has produced a patch that fully resolves this vulnerability. Aaron Portnoy has validated this patch. This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The Schneider Electric products affected:

- IGSS application, all versions.

IMPACT

An exploit of this vulnerability could result in a buffer overflow that could possibly allow an attacker to execute code under administrator credentials. IGSS is employed in many sectors including renewable energy, process control, monitoring and control, motor controls, lighting controls, electrical distribution, and security systems.

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 US-based company that maintains offices in 190 countries worldwide. Their products address various markets including renewable energy, process control, monitoring and control, motor controls, lighting controls, electrical distribution, and security systems.

IGSS is a desktop application that is used to integrate industrial control system (ICS) components from diverse vendors using diverse sets of protocols and integrate their configuration and monitoring functions using IGSS as a single supervisory or human-machine interface (HMI) system. This software is employed worldwide in a broad range of application areas outside those market areas listed above.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Vulnerability classifications are classified by Common Weakness Enumerations (CWE).[a] This stack-based buffer overflow is classified as CWE-121.

STACK-BASED BUFFER OVERFLOW[b]

IGSS communicates with a broad range of ICS devices using a broad range of protocols over two network ports, Ports (12397 and 12399)/TCP by default. This exploit has found that out-of-protocol communication over Port 12397/TCP can cause a buffer overflow condition. Although this overflow can cause the application to crash, an attacker can also apply techniques to take advantage of the buffer overflow and likely execute malicious code with administrator privileges.

CVE-2013-0657[c] 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).[d]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

a. CWE: Common Weakness Enumerations, http://cwe.mitre.org/data/, Web site last accessed January 18, 2013.
b. CWE-121, http://cwe.mitre.org/data/definitions/121.html, CWE-121: Stack-based Buffer Overflow, Web site last accessed January 18, 2013.
c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0657 , 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?name=&vector=%28AV:N/AC:L/Au:N/C:C/I:C/A:C%29&version=2 , Web site last visited January 18, 2013.

DIFFICULTY

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

MITIGATION

The best mitigation for this vulnerability is applying the appropriate vendor-supplied patch listed in the footnotes below.

Schneider Electric has issued two patches for versions V9[e] and V10[f] of the IGSS software to address this vulnerability. These patches are available from the Schneider Electric Web site or directly from the links in this advisory. Aaron Portnoy of Exodus Intelligence has validated the patches.

If this vulnerability is not mitigated, a remote attacker could cause a buffer overflow and allow malicious code to be executed with administrator privileges.

Users of this software with older versions should upgrade their software or employ other mitigation methods. At a minimum, this port should be filtered to only allow access from the specific IP addresses for the devices being controlled or monitored. General measures listed below can also be employed to help mitigate this 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 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

e. IGSS V9 Patch, http://igss.schneider-electric.com/igss/igssupdates/v90/progupdatesv90.zip , last visited January 18, 2013

f. IGSS V10 Patch, http://igss.schneider-electric.com/igss/igssupdates/v100/progupdatesv100.zip , last visited January 18, 2013

Strategies.[g] 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,[h] 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.

Previous Recommendations can be used as needed (otherwise, delete this text). List other products that are specific to the topic (i.e., phishing mitigations):

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[i] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[j] 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@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/.

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 18, 2013.

h. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed January 18, 2013.

i. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed January 18, 2013.

j. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed January 18, 2013.

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.