ICS-CERT ADVISORY

ICSA-11-273-01—ICONICS GENESIS32 MULTIPLE MEMORY CORRUPTION VULNERABILITIES

September 30, 2011

OVERVIEW

Independent security researchers Billy Rios and Terry McCorkle have identified eight memory corruption vulnerabilities affecting the ICONICS GENESIS32 product. GENESIS32 is a web-deployable human-machine interface (HMI) supervisory control and data acquisition (SCADA) product. These vulnerabilities affect ScriptWorX32, GraphWorX32, and the AlarmWorX32 and TrendWorX32 containers that run as part of the GENESIS32 application.

ICONICS has validated the reported vulnerabilities and has produced patches that address them. ICS-CERT has validated each of the patches and has confirmed that they resolve these vulnerabilities.

AFFECTED PRODUCTS

According to ICONICS, the following versions of GENESIS32 are affected:

- GENESIS32 V8.05, V9.0, V9.1, and V9.2—ScriptWorX32, AlarmWorX32 and TrendWorX32 containers
- GENESIS32 V9.2—GraphWorX32

IMPACT

Successful exploitation of these vulnerabilities results in an application crash and can allow 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 these vulnerabilities based on their environment, architecture, and product implementation.

BACKGROUND

ICONICS is a US-based company that maintains offices in several countries around the world, including the US, UK, Netherlands, Italy, India, Germany, France, Czech Republic, China, and Australia.

The affected product, GENESIS32, is a web-deployable HMI SCADA system. According to ICONICS, GENESIS32 is used primarily in the United States and Europe, with a small percentage in Asia, and is

deployed across several industries including manufacturing, building automation, oil and gas, water and wastewater, electric utilities, and others.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A total of eight memory corruption vulnerabilities were reported by the researchers. These vulnerabilities affect the ScriptWorX32, GraphWorX32, AlarmWorX32, and TrendWorX32 containers that run as part of the GENESIS32 application. These vulnerabilities can be exploited using specially crafted files that, once opened, result in a crash in the application and possible arbitrary code execution.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable. Social engineering can be used in order to convince a user to open the specially crafted file containing an exploit for this vulnerability.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill level can create a working exploit for this vulnerability. Moderate skill is needed in order to execute arbitrary code.

MITIGATION

ICONICS has released patches for each of the vulnerabilities affecting the GENESIS32 application. This patch and an updated ICONICS Whitepaper on Security Vulnerabilities are available on the ICONICS CERT website: http://www.iconics.com/certs.

Users of the GENESIS32 who wish to apply this patch can refer to the ICONICS patch that matches the version of the software they are running. ICONICS has placed a Readme file in their patch download that offers instructions on how to apply the patch. If additional support is required, users can contact ICONICS for support by e-mailing supportworx@iconics.com.

ICS-CERT encourages asset owners to 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.

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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a section for control system security related 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.*[a]

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 e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[b] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[c] for more information on social engineering attacks.

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.

a. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 30, 2011.
b. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed September 30, 2011.
c. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed September 30, 2011.