ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-182-01— ICONICS GENESIS32 AND BIZVIZ ACTIVEX TRUSTED ZONE VULNERABILITY

July 01, 2011

OVERVIEW

ICS-CERT has received a report from independent security researchers Billy Rios and Terry McCorkle concerning ICONICS GENESIS32 and BizViz products. This vulnerability involves a design issue in a GENESIS32 ActiveX control that can set an arbitrary domain to the trusted zone. ICONICS has validated the researchers’ claims for multiple versions of GENESIS32 and BizViz.

ICS-CERT has coordinated this vulnerability report with ICONICS and they have released a patch that addresses the vulnerability. The researchers have validated that the patch mitigates the reported vulnerabilities.

AFFECTED PRODUCTS

According to ICONICS, this vulnerability exists in two ICONICS products. The products and versions affected are:

- GENESIS32 – Version 9.21, including Workbench / WebHMI components
- BizViz – Version 9.21

IMPACT

Successful exploitation of this vulnerability could result in arbitrary domain intrusion into the trusted zone, introducing the potential for remote 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 the 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 products, GENESIS32 and BizViz, are web-based SCADA systems. According to ICONICS, GENESIS32 is deployed across several sectors including manufacturing, building automation, oil and gas, water and wastewater, electric utilities, and others. ICONICS estimates that these products are primarily used in the United States and Europe with a small percentage in Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Exploitation of the ICONICS GENESIS Workbench32/WebHMI component SetTrustedZone Policy vulnerability requires creation of a website that can load and use the IcoSetServer ActiveX control in a way that inserts an arbitrary domain into the Trusted Zone.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker would require at least a moderate skill level to perform a code-execution exploit of the SetTrustedZone policy vulnerability.

MITIGATION

The patch and ICONICS whitepaper are available from the ICONICS website (http://www.iconics.com/certs). ICONICS has two mitigations available for this vulnerability:

- Customers can upgrade their product to Version 9.22.
- Customers with Version 9.21 can apply the patch included with the Version 9.21 Security Updates download, which is available on ICONICS website: http://www.iconics.com/certs. ICONICS has included a “readme” file with the download that provides instructions for applying the patch.

In addition to the patch, ICONICS has also released an updated version of their “Whitepaper on Security Vulnerabilities” that includes details of this vulnerability. This document can be accessed at the following link: http://www.iconics.com/certs.

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 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*.

Use previous recommendations as needed. List the any other information products that might be specific to the topic:

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* [a] for more information on avoiding e-mail scams.
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[b] for more information on social engineering attacks.

The CSSP also provides a section for control system security 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.*[c]

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] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website accessed June 22, 2011.

[b] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website accessed June 22, 2011.

[c] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html.