ICS-CERT ADVISORY

ICSA-11-131-01—ICONICS GENESIS32 AND BIZVIZ ACTIVEX STACK OVERFLOW

May 11, 2011

OVERVIEW

Security researchers Scott Bell and Blair Strang of Security-Assessment.com[a] have released a report detailing a stack overflow vulnerability affecting ICONICS[b] GENESIS32 and BizViz products. The vulnerable ActiveX control, GenVersion.dll, is a component of WebHMI, which is incorporated in both GENESIS32 and BizViz products. Successful exploitation of this vulnerability allows remote arbitrary code execution.

ICS-CERT has confirmed that ICONICS has issued a patch that addresses this vulnerability. ICONICS confirmed that Security-Assessment.com has validated that this patch fully resolves this vulnerability.

AFFECTED PRODUCTS

According to ICONICS, GENESIS32 and BizViz (Versions 9 through 9.21) are affected by this vulnerability.

IMPACT

If successfully exploited, this vulnerability results in remote arbitrary code execution with privileges of the current user.

Actual 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 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 HMI 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 55% of GENESIS32 installations are in the United States, 45% are in Europe, and 5% are in Asia.

a. Security-Assessment.com, http://www.security-assessment.com/, website accessed May 5, 2011.
b. ICONICS, http://www.iconics.com, website accessed May 5, 2011.

VULNERABILITY (OR MALWARE) CHARACTERIZATION

VULNERABILITY (OR MALWARE) OVERVIEW

According to Security-Assessment.com, exploitation of this vulnerability requires a user with the "GenVersion.dll" ActiveX control installed to visit a web page containing specially crafted JavaScript. "GenVersion.dll" is a component used by the WebHMI interface. By passing a specially crafted string to the "SetActiveXGUID" method, it is possible to overflow a static buffer and execute arbitrary code with the privileges of the logged on user.

Users could be lured into visiting malicious sites using social engineering or phishing techniques[c].

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable using a specially crafted string sent to the "SetActiveXGUID" method.

EXISTENCE OF EXPLOIT

An exploit targeting this vulnerability is publicly available.

DIFFICULTY

This vulnerability requires moderate skill to exploit. Social engineering techniques are also needed to exploit this vulnerability.

MITIGATION

ICONICS has released a patch that addresses this vulnerability for each of the affected products. ICONICS recommends that users of GENESIS32 and BizViz install the patch entitled "WebHMI V9.21 Patch" available at: http://iconics.com/certs.

ICONICS also plans to address this vulnerability in the upcoming version 9.22 update of GENESIS32 and BizViz. ICONICS expects this update to be available in June 2011.

ICONICS has updated their "Whitepaper on Security Vulnerabilities" to include details of this vulnerability. This document is available at: http://iconics.com/certs.

For additional product support, users can contact ICONICS by phone at (508) 543-8600 or by e-mail at support@iconics.com.

c. US-CERT: Avoiding Social Engineering and Phishing Attacks, http://www.us-cert.gov/cas/tips/ST04-014.html, website accessed May 5, 2011.

ICS-CERT recommends that users also 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*[d] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[e] for more information on social engineering attacks.

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).

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 recommended practices section for control systems, on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*[f]

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.

d. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website accessed March 5, 2010.

e. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website accessed March 4, 2010.

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