ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

# ICS-CERT ADVISORY

## ICSA-12-212-01—ICONICS GENESIS32/BIZVIZ SECURITY CONFIGURATOR AUTHENTICATION BYPASS VULNERABILITY

July 30, 2012

## OVERVIEW

Dr. Wesley McGrew of Mississippi State University has identified an authentication bypass vulnerability leading to privilege escalation in the ICONICS GENESIS32 and BizViz applications, specifically in the Security Configurator component. This vulnerability allows an attacker to bypass normal authentication methods, granting full administrative control over the system. Exploits that target this vulnerability are known to be publicly available.

ICONICS has produced a hot fix that mitigates this vulnerability.

## AFFECTED PRODUCTS

Iconics reports that the zero-day vulnerability affects the following versions of Genesis32:

- Genesis32 V9.22 and previous.
- BizViz V9.22 and previous

## IMPACT

Successful exploit of this vulnerability could grant an attacker administrator privileges in the Security Configurator. This could allow the attacker to change settings in the system, including changing the rights/privileges of other users.

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

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-deployable human-machine interface (HMI) supervisory controlled and data acquisition (SCADA) systems. According to ICONICS, GENESIS32 is used primarily in the United States and Europe, with a small percentage in Asia. This product is deployed across several industries including manufacturing, building automation, oil and gas, water and wastewater, electric utilities, and others.

# VULNERABILITY CHARACTERIZATION

## VULNERABILITY OVERVIEW

### AUTHENTICATION BYPASS[a]

An attacker posing as a locked-out ICONICS GENESIS32 or BizViz user can generate an authentication code without contacting ICONICS technical support. The attacker can then login to the Security Configurator with administrative privileges and change system settings and privileges for other users.

CVE-2012-3018[b] has been assigned to this vulnerability. A CVSS v2 base score of 6.0 has been assigned; the CVSS vector string is (AV:L/AC:H/Au:S/C:C/I:C/A:C).[c]

## VULNERABILITY DETAILS

### EXPLOITABILITY

An attacker needs local access to exploit this vulnerability.

### EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

[a] CWE-261: Weak Cryptography for Passwords, http://cwe.mitre.org/data/, Web site last accessed July 30, 2012

[b] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3018, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[c] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:H/Au:N/C:C/I:C/A:C), Web site last visited July 30, 2012.

## DIFFICULTY

An attacker with moderate skill level and knowledge of the encryption algorithm used to secure the challenge response could obtain administrator privileges in the system.

## MITIGATION

ICONICS is releasing a patch for the GENESIS32 and BizViz security files for Versions 8.05, 9.01, 9.13, and 9.22 that disable the backdoor security login. In the future, this feature will be re-implemented with a more secure encryption algorithm.

ICONICS provides information and links related to its security updates for this and other patches, at its website at http://www.iconics.com/certs.

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.

The Control Systems Security Program (CSSP) also provides a section for control systems 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.[d] 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,[e] which 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.

## ICS-CERT CONTACT

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

[d] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed July 30, 2012.

[e] Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed July 30, 2012.

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP 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/.

## 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.