ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-108-01—ICONICS GENESIS MULTIPLE VULNERABILITIES

April 18, 2011

OVERVIEW

An independent security researcher has published 13 vulnerabilities with proof of concept (PoC) code[a] for the ICONICS GENESIS32 and GENESIS64 human-machine interface (HMI)/supervisory control and data acquisition (SCADA) products.

The 13 remotely exploitable vulnerabilities exploit the GenBroker.exe service on Port 38080/TCP. The researcher states that the vulnerabilities fall within two classifications: twelve involve integer overflows;[b] one involves memory corruption.[c]

After the aforementioned vulnerabilities were disclosed, a second, security researcher, Joel Langill of SCADAhacker,[d] is coordinating with the ICS-CERT on another vulnerability in the ICONICS GENESIS products. Mr. Langill reported a vulnerability in the SafeNet Sentinel License Monitor httpd 7.3 service on Port 6002/TCP, which is used by the ICONICS GENESIS32 and GENESIS64 application suites. That vulnerability is based on a previously reported vulnerability in the SafeNet Sentinel License Monitor service.[e] An attacker could exploit this vulnerability to allow directory traversal on the host machine.

ICONICS has validated the reported vulnerabilities and released a software update that addresses all identified vulnerabilities. ICS-CERT has verified that the update released by ICONICS fully addresses all reported vulnerabilities.

[a] ICS-ALERT-11-080-02, ICS-CERT, www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-080-02.pdf, accessed April 4, 2011.

[b] CWE-190: Integer Overflow, Common Weakness Enumeration, http://cwe.mitre.org/data/definitions/190.html, accessed March 31, 2011.

[c] CWE-415: Double-Free, Common Weakness Enumeration, http://cwe.mitre.org/data/definitions/415.html, accessed March 31, 2011.

[d] Joel Langill, Cyber Security to Protect Critical Infrastructure, http://scadahacker.com/, accessed April 13, 2011.

[e] CVE-2007-6483 (under review), National Vulnerability Database, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6483, accessed April 4, 2011.

AFFECTED PRODUCTS

INTEGER OVERFLOWS AND MEMORY CORRUPTION VULNERABILITIES

The Integer overflows and Memory Corruption vulnerabilities affect ICONICS GENESIS32 and GENESIS64. Versions affected are:

- GENESIS32 Version 9.21 and prior
- GENESIS64 Version 10.51 and prior.

DIRECTORY TRANSVERSAL VULNERABILITY

The directory traversal vulnerability affects all versions of GENESIS32 and GENESIS64 that utilize SafeNet Sentinel License Monitor service (Versions 7.0 through 7.4). The National Vulnerability Database (NVD) includes an unconfirmed report that versions prior to 7.0 may also be vulnerable.[e] According to ICONICS, vulnerable versions of the SafeNet service could exist in the following versions of the GENESIS application suite:

- GENESIS32 and GENESIS 64 (Versions 8.05, 9.1, 9.2, and 10)

IMPACT

An attacker successfully exploiting these identified vulnerabilities could remotely execute arbitrary code, create data leakage, or initiate a denial of service (DoS). The 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 GENESIS64, are web based HMI SCADA systems. According to ICONICS, GENESIS is deployed across several sectors including manufacturing, building automation, oil and gas, water and wastewater, electric utilities, and others. ICONICS estimates that 55% of GENESIS installations are in the United States, 45% are in Europe, and 5% are in Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The publicly disclosed vulnerabilities affect the GenBroker.exe on Port 38080/TCP, which is an OPC-based communications service. If exploited, this vulnerability provides access to a core application used to manage communications between clients and servers. This service is vulnerable to integer overflow and memory corruption conditions. All these vulnerabilities are potentially remotely exploitable.

DIRECTORY TRANSVERSAL VULNERABILITY

This vulnerability in the ICONICS GENESIS32 and GENESIS64 application suites affects the SafeNet Sentinel License Monitor service on Port 6002/TCP, through a previously reported vulnerability of that service.[e] The ICONICS GENESIS32 and GENESIS64 application suites use this service as part of product licensing. An attacker could exploit this vulnerability to allow directory traversal on the host machine, potentially gaining additional privileges that could facilitate malicious acts against the vulnerable system.

INTEGER OVERFLOWS AND MEMORY CORRUPTION VULNERABILITY DETAILS

EXPLOITABILITY

An attacker can remotely exploit all the identified vulnerabilities by sending specially crafted data to the vulnerable GenBroker.exe application. An attacker could craft a malicious payload that could be remotely executed.

EXISTENCE OF EXPLOIT

PoC code is publicly available for all 13 reported vulnerabilities.

DIFFICULTY

This vulnerability requires moderate skill to exploit.

DIRECTORY TRANSVERSAL VULNERABILITY DETAILS

EXPLOITABILITY

An attacker could remotely exploit this vulnerability by sending specially crafted data to the vulnerable SafeNet Sentinel License Monitor service on Port (6002/TCP).

EXISTENCE OF EXPLOIT

No publicly available exploit code is known to exist that specifically targets this vulnerability.

DIFFICULTY

This vulnerability requires moderate skill to exploit.

MITIGATION

ICONICS has addressed these vulnerabilities with a software update, which is available on the company's website: http://www.iconics.com/certs.

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

In addition to software updating, ICS-CERT recommends the following mitigations:

- Use a firewall to restrict unnecessary or unwanted traffic, specifically to the affected Ports 38080/TCP and 6002/TCP.
- If an intrusion detection system (IDS) is used, update to the latest IDS signatures.
- Minimize exposure of vulnerable systems to external networks. If 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 System Security Program 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 Control System Security Program 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.

[f] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, accessed March 31, 2011.