ICS-CERT ADVISORY

ICSA-11-096-01—GLEG Agora SCADA+ Exploit Pack

April 06, 2011

SUMMARY

On March 15, 2011, GLEG Ltd. announced the Agora SCADA+ Exploit Pack for Immunity's CANVAS system. CANVAS is a penetration testing framework that is extensible using CANVAS Exploit Packs. On March 25, 2011, GLEG announced it would be adding exploits for the 35 vulnerabilities released by Luigi Auriemma on March 21, 2011. The ICS-CERT has not received any reports of this tool being used for an unauthorized compromise of an actual control system installation.

ICS-CERT has prepared this advisory to provide an initial summary of the possible vulnerabilities contained in this exploit pack. Please note that at this time, the information contained in this report is not conclusive, nor is it comprehensive. This report represents a cursory and credible snapshot of the vulnerabilities that are likely contained in the pack, based on the analysis conducted by ICS-CERT.

BACKGROUND

Immunity's CANVAS is a penetration framework similar to the popular Metasploit tool. GLEG is a small company based in Moscow, Russia, that produces add-on exploit packages for Canvas. On March 22, 2011, GLEG's CEO, Yuriy Gurkin, announced that its website was under a distributed denial-of-service (DDoS) attack with traffic exceeding 100 Gb per day. The source and intent of this traffic is unknown at this time.

IMPACT

ICS-CERT contacted Immunity and obtained a general list of the targeted products and exploits (with very limited vulnerability details) contained in the Agora SCADA+ Exploit Pack. ICS-CERT has analyzed the data and surmises that of the 24 vulnerabilities, 18 are previously known and patched. One product could not be identified from the information provided. After consultation with the affected vendors, it appears that the remaining five may be true zero-day vulnerabilities. However, because the technical details of the vulnerabilities are not known, ICS-CERT's analysis is not conclusive and vendors may have a difficult time addressing and patching these suspected vulnerabilities.

ICS-CERT contacted each of the identified vendors to inform them of the GLEG product. Some vendors have reached out to GLEG directly for additional information. ICS-CERT is also attempting to work with GLEG to obtain additional information and will update this reporting it as it becomes available.

REFERENCES

ICS−ALERT-11-080-01 Multiple Vulnerabilities in Siemens Tecnomatix Factorylink

ICS−ALERT-11-080-02 Multiple Vulnerabilities in Iconics Genesis (32 & 64)

ICS−ALERT-11-080-03 Multiple Vulnerabilities ion 7-Technologies IGSS

ICS−ALERT-11-080-04 Multiple Vulnerabilities in Realflex RealWin

Table 1. Known vulnerabilities likely included in the Agora SCADA+ Pack

Product	Exploit	CVE	ICS-CERT Advisory
Indusoft SCADA web studio 7.0 heap corruption	Heap corruption	CVE-2011-0488	**
SCADA Trace Mode Data Center	File disclosure	None	**
IGSS SCADA odbc server	DoS	None	ICSA-11-018-02 – IGSS ODBC Server Remote_Heap Corruption
OPC Modbus Ethernet OPC Server	DoS	CVE-2010-4709	ICSA-10-322-02A - Automated Solutions OPC Server Vulnerability
ITS scada	SQL Injection	None	Demo website according to vendor, no ICS Product produced
Automated Solutions Modbus/TCP OPC Server	Remote Heap Corruption	CVE-2010-4709	ICSA-10-322-02—Automated Solutions OPC Server Vulnerability
BACnet OPC client before 1.0.25	Arbitrary code execution	CVE-2010-4740	ICS-Alert-10-264-01 - SCADA Engine BACnet OPC Client Buffer Overflow Vulnerability
Advantech Studio 6.1 Web server	DoS	CVE-2011-0488	ICSA-10-337-01 – Advantech_Studio_Buffer_Overflow
ICONICS Dialog Wrapper Module ActiveX control	Exploit	CVE-2006-6488	*
BECK GMBH, INDUSTRIAL PC -	IPC@CHIP DoS	CVE-2001-1340	*
BECK GMBH, INDUSTRIAL PC -	IPC@CHIP credentials stealing	CVE-2001-1341	*
SafeNet Sentinel Protection Server <= 7.4.1.0 + Sentinel Keys Server <= 1.0.4.0 DATARATE SCADA <= 2.5	Directory Traversal	CVE-2008-0760	*

Product	Exploit	CVE	ICS-CERT Advisory
SCADA MOXA Device Manager Tool 2.1	Buffer Overflow	CVE-2010-4741	ICSA-10-301-10—Moxa Device Manager Buffer Overflow
Ecava IntegraXor	Web directory traversal	CVE-2010-4598	
GE Fanuc Real Time Information Portal 2.6.		CVE-2008-0175	*
Citect SCADA ODBC	Buffer Overflow	CVE-2008-2639	*
Invensys Wonderware InFusion SCADA (and other products) ActiveX.		CVE-2010-2974	ICSA-10-208-01-Wonderware ArchestrA ActiveX Control[a]
DATAC RealWin SCADA 1.06	Buffer Overflow Exploit	CVE-2010-4142	ICSA-10-313-01—RealWin Buffer Overflows

* Vulnerability predates ICS-CERT, therefore no Advisory was published

** Vulnerability is known, but technical details are currently unknown

ZERO-DAY VULNERABILITIES

Five vulnerabilities appear to be true zero-day vulnerabilities. Because the technical details of the vulnerabilities are unknown, ICS-CERT's analysis is not conclusive and vendors may have a difficult time addressing and patching these suspected vulnerabilities. ICS-CERT has contacted the affected vendors and provided them with the available information. Some vendors have reached out to GLEG directly for additional information. ICS-CERT will continue to work with the affected vendors and will provide analysis support as needed. Also, ICS-CERT will update this report as needed.

MITIGATION

ICS-CERT recommends that asset owners and operators routinely audit their systems and apply updates as they become available or when possible. As with all system changes, administrators should consult their control systems vendor prior to making any control system changes.

Organizations observing 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 that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

a. There is no URL for this document because it was released exclusively on the US-CERT portal.

The Control System Security Program provides numerous recommended practices[b] for control systems on the US-CERT website. Several relevant recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.

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.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website accessed April 06, 2011.