ICS-CERT ALERT

ICS-ALERT-11-230-01— GLEG AGORA SCADA+ EXPLOIT PACK UPDATE 1.4

August 18, 2011

ALERT

SUMMARY

The GLEG Agora SCADA+ Exploit pack is a collection of exploits that specifically target Industrial Control Systems (ICS) products. The inclusion of exploits for vulnerabilities in ICS products increases the ease with which an attacker could exploit these products.

Users of the affected products should reference the ICS-CERT and/or CVE information available in Table 2 and act on the mitigation actions specific to the vulnerability. Users of affected products that have no complete mitigation, such as a patch, should work to implement relevant defensive measures including but not limited to defense in depth strategies.

ICS-CERT has prepared this Alert to provide a list of the vulnerabilities possibly contained in this exploit pack to foster heightened awareness of these vulnerabilities and available mitigations. Table 1 outlines existing public ICS-CERT products related to the Agora SCADA+ Exploit Pack.

Table 1. ICS-CERT products

Release Date	Product Name	Link
April 6, 2011	ICSA-11-096-01— GLEG Agora SCADA+ Exploit Pack	Link
April 21, 2011	ICS-ALERT-11-111-01—GLEG Agora SCADA+ Exploit Pack Update 1.1	Link

The information contained in this report is neither conclusive nor comprehensive since only a general list is available for the targeted products and exploits, with limited details. The information contained in Table 2 of this Alert represents a cursory and credible snapshot of the vulnerabilities that are likely included in the exploit pack, based on ICS-CERT analysis.

Table 2 below summarizes the possible vulnerabilities for which exploits are available in the Agora SCADA+ Exploit. ICS-CERT has identified 40 potential exploits.

Table 2. Exploit Pack vulnerability exploits

Vendor	Product	Vulnerability Type	CVE	ICS-CERT Product
7-Technologies	IGSS	Multiple	Unknown	ICS-ALERT-11-080-03 ICSA-11-132-01 ICSA-11-132-01A
7-Technologies	IGSS ODBC Server	Denial of Service	Unknown	ICSA-11-018-02
Automated Solutions	Modbus/TCP OPC Server	Remote Heap Corruption	CVE-2010-4709	ICSA-10-322-02
BACnet	OPC client (prior to 1.0.25)	Arbitrary code execution	CVE-2010-4740	ICS-Alert-10-264-01
Beck	IPC@CHIP	Denial of Service	CVE-2001-1340	*
Beck	IPC@CHIP	Credentials Stealing	CVE-2001-1341	*
Beckhoff	TwinCAT ENI Server 1.1.6.0	Unknown	Unknown	
Broadwin/Advantech	Studio 6.1 Web server	Denial of Service	CVE-2011-0488	ICSA-10-337-01
Broadwin/Advantech	Studio ISSymbol (prior to 7.0+SP1)	Buffer Overflow	CVE-2011-0340	ICS-ALERT-11-131-01
Broadwin/Advantech	WebAccess	Buffer Overflow	CVE-2011-0488	ICSA-10-337-01
Broadwin/Advantech	WebAccess	Multiple ActiveX Vulnerabilities	Unknown	
Broadwin/Advantech	WebAccess	Denial of Service	Unknown	
Broadwin/Advantech	WebAccess	SQL Injection	Unknown	
CACHE	Database	Denial of Service	Unknown	
CACHE	Database	Denial of Service	Unknown	
Citect	CitectSCADA ODBC	Buffer Overflow	CVE-2008-2639	*
CodeSys	ENI Server v. 1.1.4.0	Code Execution	Unknown	
DATAC/RealFlex	RealWin	Multiple	CVE-2010-4142	ICS-ALERT-10-305-01 ICSA-10-313-01

Vendor	Product	Vulnerability Type	CVE	ICS-CERT Product
DATAC	RealWin SCADA 1.06	Buffer Overflow	CVE-2010-4142	ICSA-10-313-01
ECAVA	IntegraXor 3.6.4000	SQL Injection	CVE-2011-1562	ICSA-11-082-01
ECAVA	IntegraXor	Web directory traversal	CVE-2010-4598	ICSA-10-362-01
GE	Fanuc Real Time Information Portal 2.6.	File Upload	CVE-2008-0175	*
ICONICS	Dialog Wrapper Module ActiveX control	Buffer Overflow	CVE-2006-6488	*
ICONICS	Genesis32/Genesis64 GenBroker	Denial of Service	Unknown	ICS-ALERT-11-080-02 ICSA-11-108-01
ICONICS	Genesis32/Genesis64	Multiple	Unknown	ICS-ALERT-11-080-02 ICSA-11-108-01
Indusoft	Web Studio 7.0	Heap corruption	CVE-2011-0488	ICSA-10-337-01
Indusoft	Thin Client 7.0	Buffer Overflow	CVE-2011-0340	ICSA-11-168-01
ITS	Unknown	SQL Injection	Unknown	
Invensys/Wonderware	InFusion ActiveX (and other products)	ActiveX Exploit	CVE-2010-2974	
Modbus	Ethernet OPC Server	Denial of Service	CVE-2010-4709	ICSA-10-322-02 ICSA-10-322-02A
MOXA	Device Manager Tool 2.1	Buffer Overflow	CVE-2010-4741	ICSA-10-301-01
Outlaw Automation	ICSCADA	SQL Injection	Unknown	
RealWin	Unknown	Memory Corruption	Unknown	
Safenet	Sentinel Protection Server 7.4.1.0 Sentinel Keys Server 1.0.4.0	Directory Traversal	CVE-2008-0760	*

Vendor	Product	Vulnerability Type	CVE	ICS-CERT Product
Siemens	Tecnomatix FactoryLink	Multiple	Unknown	ICS-ALERT-11-080-01 ICSA-11-091-01A
Sunway	ForceControl WebServer	Heap Overflow	CVE-2011-2960	ICSA-11-167-01
Trace Mode	Data Center	File Disclosure	Unknown	
Wellintech	Kingview 6.53	Buffer Overflow	CVE-2011-0406	ICSA-11-074-01
Wintr	Unknown	SQL Injection	Unknown	
Wintr	Unknown	SQL Injection	Unknown	

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

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ICS-CERT@DHS.GOV

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.