



APRIL 2011



INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

**Incident Response
Analysis
Announcements
Recent Product Releases
Open Source Situational
Awareness Highlights
Upcoming Events
Coordinated Vulnerability
Disclosure
Document FAQ**

ICS CYBER TIP 4 U

**Be Alert for Spear-Phishing
E-mails**

The cyber bad guys are getting better at spoofing legitimate users and targeting individuals with apparently credible e-mail messages to lure them into opening malicious files.

Unless you were expecting the e-mail, think twice about opening that attachment!

Contact Information

For any questions related to this report or to contact ICS-CERT:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting:
<http://www.ics-cert.org>

What is ICS-CERT?

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to:

- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

The “ICS-CERT Monthly Monitor” offers a means of promoting preparedness, information sharing, and collaboration with the 18 critical infrastructure/key resource (CIKR) sectors. The ICS-CERT accomplishes this on a day-to-day basis through sector briefings, meetings, conferences, and information product releases.

INCIDENT RESPONSE

The ICS-CERT works closely with industry, academia, private researchers, and law enforcement to respond to and resolve security incidents that affect industrial control systems. These incidents often provide lessons learned that apply to the overall critical infrastructure ICS community. The following is a snapshot of some of the notable incidents that ICS-CERT triaged this past month. Please note that for privacy purposes we have removed names, locations, and specific details to protect the affected entity.

Internet Facing Control Systems

This month ICS-CERT responded to multiple reports of Internet facing SCADA systems, most of them in the water and energy sectors. Some of these systems were configured with default logon credentials. Most of these ICS systems are intended to provide remote access for monitoring system status or certain asset management features. However, if not configured correctly, these systems are at greater risk for cyber attacks and intrusions.

The ICS-CERT worked closely with the affected entities, vendors, systems integrators, international partners, and the sector Information Sharing and Analysis Center (ISAC) to assist with mitigation. In all cases, the default logins were changed as a result of the notification, and the vendors and systems integrators are working together to ensure better implementation of procedures to prevent instances of this occurring in the future. This coordination provided ICS-CERT a valuable opportunity to reach out and share vulnerability mitigation strategies while partnering with the ICS community.

For more information on Internet accessibility and securing your control systems, review [ICSA-10-301-01 – Control System Internet Accessibility](#).

Malicious Cyber Activity at a Water Utility

ICS-CERT recently assisted a water utility to evaluate a reported cyber incident when remote users experienced difficulties logging into the control systems. Both offsite and onsite analyses were conducted (including malware and digital media analysis of their systems) revealing that the incident was attributed to general crimeware and not targeted. Their control systems were not impacted in the incident.

(Continued on Page 2)



Malicious Cyber Activity at a Water Utility (cont'd.)

ICS-CERT coordinated with the FBI, state, and local law enforcement during and after the incident response. While onsite, ICS-CERT reviewed network topologies and control systems architecture and evaluated their current security and detection measures. ICS-CERT provided mitigations and made recommendations for strengthening the existing cyber security and incident detection mechanisms. The customer has since sanitized its systems and implemented stronger and tighter security practices. Some of the general lessons learned include:

- Secure remote access with VPNs or two-factor authentication. For more information about configuring and managing remote access, review [Configuring and Managing Remote Access for industrial Control Systems](#).
- Prepare for incidents with a formalized incident response plan. Enable logging and leverage the static nature of a control system to look for anomalies. Retain logs for a sufficient amount of time.
- Understand how to preserve forensic data for analysis and reporting when an incident occurs. For example, capture forensic images of the system memory and hard drive prior to powering down the system. Also, avoid running antivirus software “after the fact” as the AV scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines.

Even with the best cyber defense mechanisms in place, cyber incidents will likely occur. Are you adequately prepared to identify what went wrong and to recover? For more information on incident handling and analysis, review [ICS-CERT's Incident Handling Brochure](#).

Russian Security Team Updates SCADA Exploit Tool

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.

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.

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. Please review [ICSA- 11-096-01- Agora SCADA Pack](#) for a detailed listing of the vulnerabilities and analysis.

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 report it as it becomes available.

ANNOUNCEMENTS

CSET 3.0 is Now Available for Download

Control Systems Security Program (CSSP) has improved on the original Cyber Security Evaluation Tool (CSET) to assist owners in conducting self-assessments. The CSET is a desktop software tool that enables users to assess their network and ICS security practices against recognized industry and government standards, guidelines, and practices. A completed CSET assessment provides a prioritized list of recommendations for improving the organization's ICS or enterprise network cybersecurity posture and identifies what is needed to achieve the desired level of security within the specific standards selected. CSET and associated training are available free of charge to CIKR stakeholders. Since October 2009, CSSP has distributed more than 1,000 copies to asset owners, enabling them to assess and address cybersecurity risk within their ICS environment.

The new release, CSET 3.0, includes the most recent standards, an enhanced user interface, and a graphical ICS architecture mapping capability.

For information on the CSET, visit the CSSP website at: http://www.us-cert.gov/control_systems/satool.html

RECENT PRODUCT RELEASES

In the past month, the ICS-CERT released the following products on the US-CERT public website.

[Advisory "ICSA-11-084-01—Solar Magnetic Storm Control Systems Impact"](#) describes potential impacts of solar storms on control systems and offers general mitigation strategies.

[Advisory "ICS-Advisory -11-082-01—Ecava IntegraXor Unauthenticated SQL vulnerability"](#) describes a SQL related vulnerability in this product.

[Alert "ICS-ALERT-11-081-01—BroadWin WebAccess"](#) warns users of a new publicly released RPC vulnerability.

[Alert "ICS-ALERT-11-080-01—Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink"](#) warns users of a new publicly released vulnerability in this product.

[Alert "ICS-ALERT-11-080-02—Multiple Vulnerabilities in Iconics Genesis"](#) warns users of a new publicly released vulnerability in this product.

[Alert "ICS-ALERT-11-080-03—Multiple Vulnerabilities in 7-Technologies IGSS"](#) warns users of a new publicly released vulnerability in this product.

[Alert "ICS-ALERT-11-080-04—Multiple Vulnerabilities in RealFlex RealWin"](#) warns users of a new publicly released vulnerability in this product.

[Advisory "ICSA-11-074-01—WellinTech KingView 6.53 KVWebSvr Active X"](#) describes a stack-based vulnerability in the KingView HMI.

[Alert "ICS-ALERT-11-066-01—ActiveX Vulnerability in WellinTech KingView 6.53"](#) warns users of a new publish vulnerability.

[Advisory "ICSA-11-056-01—Progea Movicon TCPUpload Server"](#) describes a data leakage and denial-of-service vulnerability in Progea's Movicon 11 HMI.

[UPDATED Advisory "ICSA-10-348-01A—Wonderware InBatch Buffer Overflow"](#) provides a link to the Invensys patch.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Why Cybersecurity Partnerships Matter

March 26, 2011

"For years, the federal government has launched one policy initiative after another to protect critical IT infrastructure in coordination with the private sector."

http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=229301141&cid=RSSfeed_IWK_All

'Low Impact' Breaches Can Signal More Badness To Come

March 25, 2011

"When is a database breach not a breach at all? If you're a stickler for the letter of the law, then perhaps it's when that breach doesn't expose regulated information, such as Social Security numbers or credit card numbers. But if your organization is a victim of a seemingly inconsequential hit that exposes items such as e-mail addresses or passwords that can be reset, it could mean more problems for you than you think."

<http://www.darkreading.com/database-security/167901020/security/attacks-breaches/229219443/>

Leader of Hacker Gang Sentenced to 9 Years For Hospital Malware

March 18, 2011

"The former leader of an anarchistic hacking group called the Elektronik Tribulation Army was sentenced Thursday to 9 years and 2 months in prison for installing malware on computers at a Texas hospital."

<http://www.wired.com/threatlevel/2011/03/ghostexodus-2/#>

The New Cyber Arms Race

March 07, 2011

"Deep inside a glass-and-concrete office building in suburban Washington, Sean McGurk grasps the handle of a vault door, clicks in a secret entry code, and swings the steel slab open."

<http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race>

Malware Attacks Decline In SCADA, Industrial Control Systems, Report Says

March 07, 2011

"Malware accounts for close to one-third of all real-world industrial control system security incidents recorded in the Security Incidents Organization's [SIO] Repository of Industrial Security Incidents (RISI) database, according to a new report published by the SIO."

<http://www.darkreading.com/insider-threat/167801100/security/attacks-breaches/229300509/>

NIST Issues Risk Management Guidance

March 03, 2011

"The federal agency for implementing technology standards has published a guide to help government organizations weave overall objectives and goals into the fabric of their security strategy."

<http://www.darkreading.com/security/news/229300172/nist-publishes-risk-management-guidance.html>

Disclaimer: The ICS-CERT compiles this section from multiple resources including current events as disclosed on websites, blogs, mailing lists, and at conferences. The ICS-CERT does not endorse the opinions or comments stated in these articles, nor has the US Department of Homeland Security (DHS) independently verified the technical information included.

UPCOMING EVENTS

April 11–15

CSSP Advanced Training

Idaho Falls, ID

<https://secure.inl.gov/ICSADV0411/>

April 12

Association of Metropolitan Water Agencies Water Policy Conference

Washington, DC

<http://amwa.net/cs/2011WPC>

April 12–13

CIP—SCADA Security Workshop

Vancouver, BC, Canada

April 17–19

American Chemistry Council: Responsible Care Conference and Expo

Miami, FL

http://www.americanchemistry.com/s_acc/sec_events.asp?CID=2456&DID=11582

April 22

Introductory Training

Honolulu, HI

http://www.us-cert.gov/control_systems/cstraining.html#workshop



DOCUMENT FAQ

What is the publication schedule for this digest? The ICS-CERT publishes the “ICS-CERT Monthly Monitor” approximately 12 times per year. Each issue includes information collected in the previous 28 to 31 days.

The public can view this document on the US-CERT website under the Control Systems link: (http://www.us-cert.gov/control_systems/).

The ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.

Please direct all questions or comments about the content, or suggestions for future content, to the ICS-CERT at ics-cert@dhs.gov.

UPCOMING EVENTS (Cont'd.)

May 02–05

ICSJWG Conference

Dallas, TX

http://www.us-cert.gov/control_systems/icsjwg/conference.html

May 23–27

CSSP Advanced Training, International

Idaho Falls, ID

http://www.us-cert.gov/control_systems/cstraining.html#workshop

May 24–26, Energy Telecommunications and Electrical Association (ENTELEC)

Houston, TX

<http://www.enteleccshow.org/>

May 25–26

Managing SCADA Security Risks 2011

San Francisco, CA

<http://www.managing-scada-security-risks.com/>

UPCOMING EVENTS (Cont'd.)

June 06–10

Advanced Training

Idaho Falls, ID

http://www.us-cert.gov/control_systems/pdf/ICS_AdvancedTrainingInvite_June6-10_2011.pdf

June 07–08

2nd Annual Smart Grid Interoperability Summit

Toronto, Ontario, Canada

<http://www.smartgridinterop.com/>

June 12–17, 23rd Annual GFIRST Conference

Hilton Vienna, Austria

<http://conference.first.org/>

June 27–28

Oil & Gas Cyber Security Summit

Houston, TX

<http://www.worldrg.com/showConference.cfm?confCode=GW11011>

COORDINATED VULNERABILITY DISCLOSURE

The ICS-CERT actively works with a variety of researchers and ICS vendors to foster coordinated vulnerability disclosure. The coordinated disclosure process allows time for a vendor to release patches and users to apply patches prior to public disclosure of the vulnerability.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact the ICS-CERT at ics-cert@dhs.gov or toll free at 1-877-776-7585.

Notable Coordinated Disclosure Good Guys

ICS-CERT appreciates working through the coordinated disclosure process with the following researchers:

- [Dan Rosenberg](#) with **Virtual Security Research (VSR)** reported an *unauthenticated Structured Query Language (SQL) vulnerability in the Ecava IntegraXor human machine interface (HMI) product.*
- [Jeremy Brown](#) reported a *data leakage and denial-of-service vulnerability in Progea's Movicon 11 HMI product.*
- [Rubén Santamarta](#) notified ICS-CERT of a *RPC vulnerability in BroadWin WebAccess, a web browser-based HMI product.*