ICS-CERT MONTHLY MONITOR

MAY 2011

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

## CONTENTS

## MONTHLY CYBER TIP

**Working with Vendors**

Owners should establish policies for monitoring and control of vendor accounts based on recommended security practices. By following company security procedures, you can avoid malware infections.

**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 Systems 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 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.

This publication highlights recent activities and information products affecting industrial control systems (ICS) and provides a look ahead at upcoming ICS related events.

## INCIDENT RESPONSE

*ICS-CERT works closely with industry, academia, private researchers, and law enforcement to respond to and resolve security incidents that affect industrial control systems (ICSs). 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. For privacy purposes, we have removed names, locations, and specific details to protect the affected entity.*

ICS-CERT has recently responded to a number of incidents ranging from a successful spear-phishing campaign to a near miss concerning a malicious file almost copied to a control system network from infected removable media. Many incidents to which ICS-CERT responds continue to involve known threat actors and previously reported attack vectors, including inadequate security practices. The continued appearance of these common threat vectors demonstrates the importance of employing a sound "defense-in-depth" cybersecurity strategy to protect critical infrastructure control systems.

### USB Near Miss

In late April, an asset owner reported to ICS-CERT a near miss with an infected USB drive. A vendor technician was visiting the owner's facility to install a software update. Because the technician did not have administrative access to the system, he handed the USB drive containing the software update to an employee and asked the employee to copy the files to the control system. The employee followed established policy and performed an "on demand" virus check on the USB drive, which resulted in detection of a malicious file hidden in the USB drive's root folder. The technician had no idea his USB drive was carrying malware.

Because the employee followed the proper procedure, the employee averted what could have been a nasty infection of the control system network. This situation demonstrates again the importance of employing sound cybersecurity policies and practices and training staff to execute them consistently.

*(continued on page 2)*

## ANALYSIS

### Exposure of Internet Accessible Control Systems Using Search Engines

As noted in the April issue of the ICS-CERT Monthly Monitor, ICS-CERT is receiving an increasing number of reports about incidents relating to Internet-facing control systems. Researchers using specialized Internet search engines, such as SHODAN and the Every Routable IP Project (ERIPP),[c] have discovered the majority of these identified control systems. Several of these identified control systems were also using default or otherwise insecure credentials, making them extremely vulnerable to unauthorized access.

Specialized search engines originated as network engineering tools; they are designed to help identify all Internet-facing devices,[d] including control system devices. These search tools scan the entire Internet for specific services using HTTP, HTTPS, Telnet, SMTP, SSH, and FTP (all common services used by control systems). The search capabilities of these search engines also allow for specific ports, services, terms contained in network responses, locations, and other queried search criteria. When properly phrased, these queries can result in the identification of Internet-facing critical control system applications such as supervisory control and data acquisition (SCADA) and human-machine interfaces (HMI).

When a control system is identified on the Internet, it immediately becomes a potential target for attacks such as account brute forcing[b] and unpatched vulnerability exploitation. Owners and operators of control systems are advised to minimize control system exposure to the Internet while employing recommended security practices such as auditing network traffic, collecting network logs, and configuring networks for proper defensive operations (defense-in-depth).[a]

ICS-CERT recommends locating control system networks and remote devices behind properly configured and tested firewalls, and isolated from the business IT network. When remote access is required, use a secure method, such as Virtual Private Networks (VPNs), recognizing that the VPN connection is only as secure as the devices at each end.

In addition, network administrators should audit current user access rights on a regular basis to ensure terminated credentials are immediately removed.

## INCIDENT RESPONSE

*(from page 1)*

### Internet-Facing Control Systems

ICS-CERT was notified by a researcher of an Internet-facing building automation control system, which was configured to allow access using vendor's default credentials. ICS-CERT contacted the building owner and learned that the default credentials had been changed, but were later returned to the default settings at the request of the system vendor. The system vendor had made the request to maintain remote support access. The building owner has since permanently changed the default credentials to provide better security against unauthorized access.

This incident highlights a common insecure practice employed by many control system vendors who configure a remote access "back door" to their SCADA installations. The vendors use this back door for system maintenance and technical support (e.g., update software, perform maintenance, and troubleshoot issues). While the practice can benefit owners and vendors from a support perspective, it also increases the potential for unauthorized remote access to the system.

When a control system is identified on the Internet, it immediately becomes a potential target for a variety of attacks such as account brute forcing,[b] and exploitation of unpatched vulnerabilities. ICS-CERT recommends that owners and operators minimize control system exposure to the Internet by locating control system networks and remote devices behind properly configured and tested firewalls, and isolated from the business IT network. ICS-CERT also recommends that owners establish policies requiring strong passwords, the removal or change of vendor default credentials that could allow unauthorized system access, and monitoring and control of vendor accounts on control systems. For more information, please review ICSA-10-228-01—Vendor Admin Accounts Warning.

### Spear-Phishing Attack

In late April, a spear-phishing attack seriously impacted a federal government facility. Several employees at the facility were lured into clicking a link in the bogus e-mail that contained malware, which spread rapidly and extensively across the business IT network.

Fortunately, firewalls between the business IT and control system networks reportedly prevented the malware from spreading into the control systems.

This incident highlights two important concepts. First, cybersecurity training is critically important to avoid social engineering attacks like spear phishing. Second, a network layout that employs the recommended "defense-in-depth" strategies is essential to minimize the impact of an intrusion when it occurs.

Control system owners can learn more about improving their cybersecurity posture and protecting control systems by reviewing the DHS Control Systems Security Program (CSSP) Recommended Practice, "Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies," available for download at the CSSP web page.[a]

[a] http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html#nogo

[b] http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-SSH%20SCANNING.pdf

[c] http://eripp.com/

[d] http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf

## ANNOUNCEMENTS

### Catalog of Control Systems Security: Recommendations for Standards Developers, Rev 7 is Now Available for Download

The Control Systems Security Program (CSSP) has updated, revised, and published the "Catalog of Control Systems Security: Recommendations for Standards Developer, Revision 7" (CoR). This catalog combines fifteen established industrial control system security standards into one volume, guiding new and experienced owners and operators to view, compare, and evaluate existing security control elements against their particular operational requirements. Two existing standards were added to the comparison crosswalk: 1) the Consensus Audit Guideline for 20 Critical Controls and 2) NRC Regulatory Guide 5.71. In addition, CSSP reviewed and updated two standards: 1) API1164 Second Edition and 2) NERC CIPS 3. A new feature of the updated CoR is the inclusion of specific reference sections in five major standards for each control element in the catalogue. These five standards are: 1) NIST SP800-53r3; 2) Consensus Audit Guideline for 20 Critical Controls v2.3; 3) API 1164, Second Edition; 4) NERC CIPS revision 3; and 5) NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities."

The CoR also identifies and list standards, guidance, and certification documents that pertain to specific industrial critical infrastructure sectors for further user reference.

For information on the CoR, visit the CSSP website at:

http://www.us-cert.gov/control_systems/csdocuments.html.

## RECENT PRODUCT RELEASES

### ICSA-11-119-01—7-Technologies IGSS

This Advisory describes a remote stack overflow vulnerability affecting 7-Technologies (7T) Interactive Graphical SCADA System (IGSS).

### Alert ICS-ALERT-11-111-01—Agora Plus

On April 21, 2011, GLEG Ltd. announced update Version 1.1 for the Agora SCADA+ Exploit Pack for Immunity CANVAS system.

### Advisory ICSA-11-110-01—RealFlex RealWin Multiple Vulnerabilities

ICS-CERT has received a report of multiple attack vectors that can successfully exploit vulnerabilities in RealFlex RealWin. RealFlex has created and released Version (2.1.12) that resolves these issues.

### Advisory ICSA-11-103-01—Honeywell ScanServer ActiveX Control

A vulnerability was discovered in Honeywell's Web Toolkit leading to arbitrary code execution. Honeywell has confirmed and released a patch to address this issue.

### Advisory ICSA-11-094-01—Wonderware InBatch ActiveX Buffer Overflow

ICS-CERT has received a report regarding a buffer overflow vulnerability in a Wonderware InBatch Client ActiveX control.

### NCCIC Advisory—Targeted Phishing Attacks

This advisory provides general guidance to public and private sector organizations on triggering targeted phishing attacks (often referred to as spear phishing) and to offer suggested methods that minimize the possibility of a successful attack.

### Advisory ICSA-11-096-01—Agora SCADA+

On March 15, 2011, GLEG Ltd. announced the Agora SCADA+ Exploit Pack for Immunity's CANVAS system, a penetration testing framework that is extensible using CANVAS Exploit Packs.

### Advisory ICSA-11-091-01A—(UPDATE) Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink

An independent researcher has identified six vulnerabilities in the Siemens Tecnomatix FactoryLink supervisory control and data acquisition (SCADA) product.

### Advisory ICSA-11-094-02—BroadWin WebAccess RPC Vulnerability

Independent security researcher Ruben Santamarta has identified details and released exploit code for a Remote Procedure Call (RPC) vulnerability in BroadWin WebAccess, a web browser-based human machine interface (HMI) product.

### Advisory ICSA-11-091-01—Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink

An independent researcher has identified six vulnerabilities in the Siemens Tecnomatix FactoryLink Supervisory Control and Data Acquisition (SCADA) product.

## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

### Hyundai Motor steps up measures against cyber attacks

April 22, 2011

Hyundai Motor Co., Korea's leading automaker, is intensifying its security measures to fend off any cyber attack following a recent one on a major local bank that crippled the lender's operations for days, company officials said Friday.

http://m.koreatimes.co.kr/www/news/biz/2011/04/123_85670.html

### 2011 Data Breach Investigation Report

April 21, 2011

Verizon 2010 Data Breach Investigations Report Offers New and Expanded Insights into Cybercrime.

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

### Malware and other cyber threats, many of which are state sponsored, are growing

April 20, 2011

The wild, wild Web grows ever wilder, and U.S. companies and critical infrastructure remain vulnerable targets, executives from cybersecurity giant McAfee warned Wednesday.

http://www.nextgov.com/nextgov/ng_20110420_3403.php

### Cyber Warfare a new kind of war for 21st Century

April 20, 2011

Chinese hackers pose serious danger to U.S. computer networks

http://my.telegraph.co.uk/abdulmuhd/amuhd/445/cyber-warfare-a-new-kind-of-war-for-21st-century/

### Iran: "U.S. Power Grid Prime Target for Cyber Attack"

April 20, 2011

Reports indicate a recent meeting of Iran's cyber warfare leaders concluded that our grids should be their primary target.

http://pajamasmedia.com/blog/iran-u-s-power-grid-prime-target-for-cyber-attack/

### In the Dark "Crucial Industries Confront Cyber Attacks"

April 19, 2011

This is a McAfee report that covers the state of issues facing Critical Infrastructure Industries.

http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

### Critical infrastructure firms hit by DoS attacks and extortion

April 19, 2011

Eighty per cent of critical infrastructure organizations, including oil, gas, water and power companies, have been hit by a denial-of-service attack in the past year.

http://www.v3.co.uk/v3-uk/news/2044274/critical-infrastructure-firms-hit-dos-attacks-extortion

### Three Of Four Energy Firms Had Data Breach In Last Year

April 05, 2011

Three quarters of global energy corporations have suffered one or more data breaches in the last 12 months, according to a new survey by The Ponemon Institute, which finds evidence of widespread shortcomings in the energy and utilities vertical.

http://threatpost.com/en_us/blogs/study-three-four-energy-firms-had-data-breach-last-year-040511

### Anatomy of an Attack

April 01, 2011

The investigation into this attack continues but I'm eager to share some information with you about it.

http://blogs.rsa.com/rivner/anatomy-of-an-attack/

### Utilities bear heavy cost of securing infrastructure

April 01, 2011

No one knows these critical systems better than the owner operators. It is also true that no one knows the true state of cyberattacks and the cyber weapons used in these attacks better than our defense and intelligence organizations. We must also consider the role of Congress in this. Collaboration and cooperation among all those stakeholders is essential if we are to rapidly and economically deal with the threat of cyberattacks on the power grid and the rest of our critical infrastructure.

http://defensesystems.com/articles/2011/03/29/digital-conflict-utilities-struggle-with-protection-burden.aspx

***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. The links provided were confirmed at the time of data capture. ICS-CERT is not responsible for broken or non-functioning URLs.*

# UPCOMING EVENTS

## MAY

**San Diego Association of Governments (SANDAG) Regional Transportation Planning Agency – San Diego, Ca**

May 12, 2011

San Diego, CA

**Managing SCADA Network Security Risks 2011**

May 25–26, 2011

San Francisco, CA

**2011 American Gas Association Operations Conference and Biennial Exhibition**

May 24–27, 2011

Nashville, TN

**Managing SCADA Security Risks 2011**

May 25–26, 2011

San Francisco, CA

## 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 month.

The public can view this document at the ICS-CERT web page: http://ics-cert.org.

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.

## JUNE

**2nd Annual SmartGrid Technology Conference 2011**

June 1–2, 2011

San Jose, CA

**American Water Works Association (AWWA)–Ohio Section**

Introduction to Controls System Security Training

June 1, 2011

Toledo, OH

**Advanced Training: Control Systems Cyber Security Advanced Training and Workshop**

June 6–10, 2011

Idaho Falls, ID

**2nd Annual Smart Grid Interoperability Summit**

June 7–8, 2011

Toronto, Canada

**American Water Works Association (AWWA) – 2011 Annual Conference**

June 12–16, 2011

Washington, DC

**23rd Annual FIRST Conference**

June 12–17, 2011

Vienna, Austria

**2011 Rail Conference**

June 12–15, 2011

Boston, MA

**Oil & Gas Cyber Security Summit**

June 27–28, 2011

Houston, TX

**Joint Critical Infrastructure Protection (JCIP) Symposium**

June 28, 2011

Newark, NJ

## JULY

**2011 Chemical Sector Security Summit**

July 6–8 2011

Baltimore, MD

**Joint Critical Infrastructure Protection (JCIP) Symposium**

July 20–21, 2011

Atlanta, GA

## COORDINATED VULNERABILITY DISCLOSURE

*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 ICS-CERT at ics-cert@dhs.gov or toll free at 1-877-776-7585.*

### Notable Coordinated Disclosure

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

- Dillon Beresford, with NSS Labs, reported to ICS-CERT a path traversal vulnerability in the AnyMacro Mail Server.
- Joel Langill, of SCADAhacker.com, reported zero-day exploits relating to directory traversal in several ICS SCADA products.
- Steven James, of xsploited security, notified ICS-CERT of a vulnerability allowing remote code execution in AGG OPC SCADAViewer.