ICS-CERT MONTHLY MONITOR

SEPTEMBER 2011

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

CYBER TIP

DON'T CLICK ON THAT LINK!

If you do not recognize where the e-mail is from, who is sending it to you, or understand why a link has been sent to you, don't click that link or open that attachment. One false click on an innocent link can lead to a major breach in your cyber defenses. Check with your computer security department to see if it is legitimate.

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 (CSSP) 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 and key resource (CIKR) sectors. 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—SPEAR PHISHING

New Spear-Phishing Campaign Targets Nuclear and Energy

Once again, spear phishing was the dominant incident activity in August, with a new round of attack campaigns launched at critical infrastructure owners and operators. The most recent campaign appeared to target energy, nuclear, and government although it is possible that other sectors were also affected. Unique to this round of attacks was the apparent targeting of control system engineers; however, personnel in various other roles also received spear-phishing e-mails.

ICS-CERT received multiple reports from impacted organizations, analyzed various malware artifacts, and correlated all related data to determine that the attacks were part of a focused campaign. Two Alerts were issued to industry partners to warn of this activity and provide compromise indicators derived from analysis of the malware embedded in the e-mail attachments. ICS-CERT posted the Alerts on the US-CERT Control Systems Center secure portal and also disseminated them to sector organizations and agencies to ensure broad distribution to asset owners and operators. While ICS-CERT strives to make as much information publicly available as possible, the indicators in these Alerts are considered sensitive and cannot be disseminated through public or unsecure channels.

Asset owners/operators who would like access to the portal or to the Alerts can contact ICS-CERT at ics-cert@dhs.gov. Alternatively, they can work with their sector Information Sharing and Analysis Center (ISAC) or sector source for cyber alerts and information sharing to obtain the ICS-CERT Alerts.

In this particular campaign, reporting organizations enabled ICS-CERT to analyze the data and create an overall view of the activity in progress. This would not have been possible without the active cooperation of the reporting organizations, so ICS-CERT commends those involved and requests continued private sector reporting whenever possible.

For more information about recognizing and mitigating spear-phishing attempts, visit last month's Monthly Monitor and a list of resources at:

http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Jul-Aug2011.pdf.

Contingency Planning: Are You Ready for an Emergency?

Earthquake and Hurricane Batter the East Coast

Just as cyber events can manifest physical consequences, so also can physical events affect cyber systems. Emergency preparedness and contingency planning are essential to the continuity of operations for the nation's critical infrastructure. This was never clearer than when an earthquake struck portions of the mid Atlantic and Northeastern United States, followed closely by hurricane Irene during the week of August 21, 2011. While the earthquake was considered powerful by East coast standards (5.8 magnitude), no major injuries were reported, and damages appear to have been minimal. Irene was a different story, causing major flooding and wind damage along the northeastern seaboard of the US and resulting in at least 44 deaths in 10 states. According to various news outlets, Irene may be one of the costliest catastrophes in recent US history, with property damage estimates running as high as $10 billion because of the unusually large area affected by the storm.

An All Hazards Approach

ICS-CERT, as a component of the National Cybersecurity and Communications Integration Center (NCCIC), provided around-the-clock coverage during the hurricane to monitor, evaluate, and respond to issues affecting critical infrastructure and key resources (CIKR). This all hazards approach toward the security and resiliency of CIKR was conducted in coordination with the National Coordinating Center (NCC), the operational arm of the National Communications System (NCS), responsible for coordinating the restoration and the reconstitution of telecommunications services or facilities under all conditions of crisis or emergency. The ICS-CERT maintained close vigil to monitor the events and fuse together incoming data in near real-time to prepare for and respond to impacted organizations.

The major lesson learned from these two disasters is the importance of emergency preparedness and contingency planning. Organizations, particularly those that operate industrial control systems, should be practiced and prepared to implement contingency plans for emergency response and a rapid return to operation.

Well-established contingency plans should cover the following topics and include specific procedures for employees in the event of disrupted operations:

- Plans for immediate actions (e.g., should certain systems be taken off-line to avoid damage or long-term impacts)
- Communication paths (e.g., who is notified first, second, call trees with current information)
- Decision paths (e.g., who is in charge of which functions, who can make decisions)
- Methods for maintaining communication between responders (e.g., private, local, state, and federal agencies)
- Alternative continuity of operations (COOP) facilities or procedures
- Process and network configuration data preservation for restoration purposes (backups)
- Restoring affected systems after an incident/event
- Implementation of alternative processes when systems are compromised
- Employee training for contingency plans.

These recent events underscore the need to be prepared for the unexpected and to regularly test, review, and exercise standing contingency procedures for situations where preparation time is possible. A lack of preplanning and training could result in poor decisions when facing an emergency.

The National Institute of Standards and Technology (NIST) has produced Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" (Revision 3, updated May 2010), which provides guidance and recommended security practices for implementing contingency plans. ICS-CERT encourages the control system community to consider the need for developing and implementing contingency planning.

DHS also provides a document comparing fifteen complementary standards for various sectors titled "Catalog of Control System Security: Recommendations for Standards Developer" (Revision 7, April 2011).

ANNOUNCEMENTS

ICSJWG Fall Conference 2011—Vulnerability Disclosure Panel Discussion

ICSJWG will hold its fall conference in October (see Upcoming Events). ICS-CERT will be participating in a panel discussion on the topic of SCADA system vulnerability disclosure policy.

"2011 CWE/SANS Top 25 Most Dangerous Software Errors" Available for Download

MITRE, with support from the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security, maintains the Common Weakness Enumeration (CWE) website. The website provides detailed descriptions of common programming, design, and architectural errors that can render software vulnerable to exploit.

MITRE and the SANS Institute, collaborating with software security experts across the U.S. and Europe, have produced a document detailing the top 25 dangerous software errors along with useful mitigation recommendations.

The "2011 CWE/SANS Top 25 Most Dangerous Software Errors" (PDF) is an update to the 2010 listing and may be downloaded from the MITRE website:

http://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.pdf.

Transportation Sector News

The Transportation Security Administration (TSA) is hosting the second annual Cyber Security in Transportation Summit, open to Transportation Systems Sector Cyber Working Group (TSSCWG) participants and Transportation Systems Sector stakeholders. The summit will focus on cybersecurity threat awareness, recommended practices, and building public/private partnership approaches to mitigating cyber system risks in transportation systems. For more information on the summit, follow the links in the ***"Upcoming Events"*** section.

The ICSJWG—Cross-Vendor Working Group Holds Kickoff Meeting

As reported in the previous Monthly Monitor, the Industrial Control Systems Joint Working Group (ICSJWG) has formed a task team under the Vendor Subgroup to develop a unified approach for addressing serious security issues that exist across many vendor platforms used in industrial control systems today.

The task team held a kickoff meeting (conference call) on September 1, 2011. Representatives from major vendors and asset owners participated. Eric Cosman (Dow Chemical, ICSJWG Vendor Subgroup co-chair)) and ICS-CERT led the discussion covering the following:

- An inaccurate perception exists that the vendor community does not fully understand control system security challenges. However, Vendor Subgroup members vocalized that they are fully aware of the security issues facing control systems and have been actively discussing those challenges in the group's monthly meetings since inception. Eric Cornelius (DHS/CSSP/ICS-CERT) led the discussion on various related topics including the use of open protocols that lack security features needed in today's interconnected world.
- The kickoff of the development of the position paper which will define specific control system security issues and include consensus-based solutions that can be applied globally across the participating vendor community and industrial control systems landscape. The group intends for the paper to cover the core challenges faced by all vendors. Work on the draft document has begun and the Vendor Subgroup will hold a progress meeting during the ICSJWG Fall Conference in October.

ICS-CERT and the ICSJWG are encouraged by the solid response and offers of assistance from the ICS community at large. For more information or to express interest in participating, please e mail ICS-CERT at ics-cert@dhs.gov.

SECTOR SECTION

Transportation Sector

The Department of Homeland Security Transportation Security Administration (TSA) is the Sector Specific Agency (SSA) assigned to the transportation sector and publishes a weekly newsletter titled "This week in Transportation Cyber Security." This newsletter contains timely open source articles concerning current cybersecurity events in transportation. Also this month, the newsletter contains information about the 2nd Annual Cyber Security in Transportation Summit, scheduled for November 1−2, in Arlington, Virginia. This group also hosts the Transportation Systems Sector Cyber Working Group (TSS-CWG), which coordinates and assists cybersecurity development for transportation elements. To subscribe to the newsletter, or for further information about the working group's mission, e-mail CyberSecurity@tsa.dhs.gov or contact Kelley Bray, Branch Chief, CSAO, at: 571-227-2198.

We Want to Hear from You

A key aspect of our mission is providing cybersecurity products and services to ICS stakeholders. As we develop and prepare new products for our customers, we want your input. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Suggestions for improving our current products are also welcome. Please help us with your feedback as we work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to ics-cert@dhs.gov.

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-Alert-11-238-01A - (UPDATE) Sunway Force Control SCADA 6.1 SEH"

This Alert Update clarifies the status of the vulnerability as previously discovered and patched.

Alert "ICS-Alert-11-238-01 - Sunway Force Control SCADA 6.1 SEH"

ICS-CERT is aware of a structured exception handler (SEH) overwrite vulnerability in Sunway Force Control SCADA Version 6.1. Boundary errors that occur during various functions can cause heap-based or stack-based buffer overflows, which in turn may allow execution of arbitrary code.

Alert "ICS-ALERT-11-230-01 - Agora SCADA+ Update 1.4"

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.

Alert "ICS-ALERT-11-204-01B - (UPDATE) S7-300 Hardcoded Credentials"

This Alert Update clarifies the nature of the hardcoded credentials identified by the researcher and the affected PLCs.

On July 23, 2011, an independent security researcher publicly announced a vulnerability affecting the Siemens S7-300 and S7-400 PLCs. The researcher claims that he was able to achieve a command shell using credentials he was able to acquire from the PLC.

ADVISORIES

Advisory "ICSA-11-223-01A - (UPDATE) Siemens SIMATIC PLCs Reported Issues Summary"

This Advisory Update corrected a typographical error detected in the original Advisory.

Advisory "ICSA-11-103-01A - (UPDATE) Honeywell ScanServer ActiveX Control"

This Advisory Update provides researcher attribution and clarification of exploit existence.

A security research company, Secunia, has released a report of a use-after-free vulnerability in the ScanServer ActiveX control, including proof-of-concept (POC) exploit code.

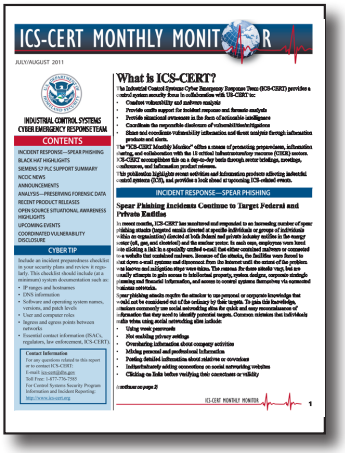
Advisory "ICSA-11-223-01 - Siemens SIMATIC PLCs Reported Issues Summary"

Beginning May 2011, ICS-CERT received multiple reports of issues affecting various models within the Siemens SIMATIC Step 7 (S7) programmable logic controller (PLC) product line.

OTHER

The ICS-CERT Monthly Monitor Jul-Aug 2011 issue

includes highlights of activities from June and July.


ICS-CERT MONTHLY MONITOR

JULY/AUGUST 2011

What is ICS-CERT?

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CONTENTS

INCIDENT RESPONSE—SPEAR PHISHING

BLACK HAT HIGHLIGHTS

SIEMENS S7 PLC SUPPORT SUMMARY

NCCIC NEWS

ANNOUNCEMENTS

ANALYSIS—PRESERVING FORENSIC DATA

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

CYBER TIP

INCIDENT RESPONSE—SPEAR PHISHING

Spear Phishing Incidents Continue to Target Federal and Private Entities

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

ICS-CERT compiles this section from multiple resources including current events as disclosed on websites, blogs, mailing lists, and at conferences. 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 nonfunctioning URLs.

Transparent cybersecurity:
Protect plant-floor data without limiting industrial network access.

August 17, 2011

"Much like a waterfall, data cascades through an organization, spilling from the plant floor and pooling where it's needed, whether that's the maintenance staff or the executive boardroom."

http://www.plantservices.com/articles/2011/08-transparent-cybersecurity-plant-floor-data-network.html

Baking Security Into Open WiFi Networks
New approach lets WiFi networks remain open and secure

August 22, 2011

"What if you could make the coffee shop wireless LAN both open and secure? That's just what a group of researchers hopes to do with their new open-source code available to organizations or establishments hosting their own WiFi networks."

http://www.darkreading.com/authentication/167901072/security/news/231500516/baking-security-into-open-wifi-networks.html

7 Controls for Mobile Devices Accessing Networks

August 22, 2011

"Elayne Starkey (Delaware state chief information security officer) is having her cake and eating it, too."

http://blogs.govinfosecurity.com/posts.php?postID=1042

Power Firms Prepare for Irene, Warn of Outages

August 25, 2011

"Power companies on the Eastern seaboard braced for Hurricane Irene, warning customers that major power outages are likely if the storm makes good on its threat to make landfall this weekend with high wind speeds."

http://online.wsj.com/article/SB10001424053111904787404576530841659014236.html?mod=googlenews_wsj

UPCOMING EVENTS

SEPTEMBER

2011 Applied Control Solutions (ACS) Conference
September 20–22, 2011
Washington Hilton
Washington, D.C.

The Cyber Security for Energy Delivery Conference
September 27–28, 2011
Crowne Plaza Hotel
San Jose – Downtown
San Jose, CA

OCTOBER

NERC GridSecCon 2011
October 18–20, 2011
JW Marriott
New Orleans, LA

Industrial Control Systems Joint Working Group (ICSJWG) 2011 Fall Conference
October 24–27, 2011
Westin Long Beach Hotel
Long Beach, CA
Register for Training

NOVEMBER

2011 TSA Cyber Security in Transportation Summit
November 1–2, 2011
Sheraton Crystal City
Arlington, VA 22202
Registration: https://www.signup4.net/public/ap.aspx?EID=TSAC10E&OID=130
Contact: cybersecurity@tsa.dhs.gov

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop (1 week)
November 7–11, 2011
Control Systems Analysis Center
Idaho Falls, ID 83415
Registration

DECEMBER

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop (1 week)
December 5–9, 2011
Control Systems Analysis Center
Idaho Falls, ID 83415
Registration

SANS Cyber Defense Initiative 2011
December 9–16, 2011
Hilton Washington & Towers
Washington, DC
Registration

DOCUMENT FAQ

What is the publication schedule for this digest?

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.

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

The public can view this document on the ICS-CERT web page at: http://www.us-cert.gov/control_systems/ics-cert/.

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

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.

Researchers Currently Working with ICS-CERT

ICS-CERT appreciates the following researchers who continue to work through the coordinated disclosure process:

Ruben Santamarta
Kuang Chun Hung (ICST)
Jeremy Brown
Billy Rios
Joel Langill
Yun Ting Lo (ICST)
Dillon Beresford
Terry McCorkle
Carlos Mario Penagos Hollmann
Michael Orlando
Knud Erik Hojgaard (nSense)
Secunia