ICS-CERT MONTHLY MONITOR

March 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

INTERESTING INCIDENT FROM FEBRUARY

SITUATIONAL AWARENESS

CSSP NEWS

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

CYBER TIP

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

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

INTERESTING INCIDENTS FROM FEBRUARY

Social engineering provides an effective means for attackers to gain access to systems. While many social engineering attempts, such as those that we receive in our inbox every day in the form of spam and phishing emails are easy for most to recognize, these attempts can also be highly targeted and conducted in a way that is much more difficult to detect. Phone-based social engineering attempts were recently experienced at two or more power distribution companies.

The utilities received a call from a representative of large software company – yes, that one that sold them the operating system on their computers –warning them that their PCs had viruses and to "Please take the following steps so I can help you correct the problem." The calls purported to be from the "Microsoft Server Department" informing the utilities that they had a virus. Of course, it wasn't really Microsoft calling, but rather an attacker, attempting to socially engineer the utilities to gain access to their systems.

The caller tried to convince the transmission managers to start certain services on their computer (likely, those services would have allowed unauthorized remote access). Fortunately for the customers of those utilities, the transmission managers recognized the social engineering attempts, refused to comply, and hung up.

This event points out the need for continued vigilance for everyone involved in critical infrastructure, particularly regarding recognition of social engineering attempts. If you are unsure whether the request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided in a URL or link connected to the request; instead, check previous statements or go to the website directly for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

ICS-CERT recommends that organizations remind users to review US-CERT TIP Avoiding Social Engineering and Phishing Attacks to learn more about what to look out for and what to do if you have fallen victim to this.

If you have experienced something similar or think you have revealed sensitive information about your organization, ICS-CERT recommends reporting it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity. In addition, immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future. ICS-CERT also encourages reporting these incidents to ICS-CERT or your local ISAC's for tracking and correlation.

ICS-CERT issued an alert on the US-CERT Secure Portal warning asset owners and operators of this observed activity. ICS-CERT often releases information pertaining to a wide variety of threats on the US-CERT Secure Portal as well as to the ICS-CERT public web page. Asset owners and operators can request access to this vetted access portal by e-mailing ICS-CERT@dhs.gov.

EVENT AUDITING AND LOG MANAGEMENT

During the lessons learned review of the 2011 fly-away events, ICS CERT found that ineffective auditing and logging was one of the most consistent technical issues/obstacles encountered when responding to onsite incident visits.

Without properly configured auditing and logging practices in place, incident response teams often find it difficult to determine the significance of a cybersecurity event. Properly configured audit logs at network, host, and application levels provide critical information for determining how an incident occurred, what the impact and scope of the issue entailed, and how best to deter future events.

The ICS-CERT has provided a collection of information resources regarding system event auditing and log management to assist vendor and asset-owner security teams to improve their current audit and logging capabilities. A list of these resources can be found at the end of this article.

Most Common Failures Associated with System Auditing and Logging

Cybersecurity teams always drive the need for robust event auditing and log management in order to support their incident response process. This is particularly true at network level events with the deployment of network intrusion detection systems (NIDS). As the type, origin, and sophistication of attacks against computer networks has changed significantly, changes in techniques for auditing and logging for host, application, data store, user access control requires significant upgrades as well to improve network data monitoring to be able to detect advanced intrusion attempts.

Comprehensive log management and analysis policy should establish minimum security audit requirements for devices, operating systems, applications, and user access control. It should also incorporate the establishment of functional best practices and minimum requirements for auditing and logging information regarding data baseline traffic for normal and off-normal operational data traffic performance. Such holistic approaches to event auditing and logging drive the centralization of data collection. This allows security, process control, and IT operations teams to easily isolate unusual data traffic based on aggregate analysis from one location for functional, operational, and security-impacting events.

A comprehensive log management and analysis program centralizes data collection from network devices, individual system operating systems, COTS applications like databases, and complex software environments like control system networks or proprietary application deployments. When configured and analyzed correctly, these data can assist in predicting equipment failure, equipment capacity, and failure points as well as providing security information.

Ineffective Log Management and Analysis Policies

Inconsistent application of even the best practices decreases their value. For example, using a standard COTS tool configured for default log management and analysis will not provide full range and benefit to the organization if the IT and ICS staffs do not understand each others' operational needs to collaborate on the configuration of audit policies (functional and security) on applications and devices. When systems and applications aren't properly configured for auditing key events, administrative and security teams do not have effective logs to review during an event (ie important event data is not captured).

Default Audit and Logging Configurations Impede Data Gathering.

Newer operating systems and applications perform more detailed configuration and event auditing options. However, the default configuration for most operating and application logs provides minimal auditing and alerting, meaning critical events don't get recorded to the event logs. Administrators must review what information they want to see and configure systems and applications to identify and record those additional events.

Default application and operating system logging configurations typically allow historical data to be overwritten after the log file has grown to a certain percentage of drive space. Without review and file management, these files will grow without bound. Scripts designed to export logs routinely from the systems to a central log management server can prevent critical information from being overwritten. In addition, current log management tools can automate log review from multiple systems, which represents a huge improvement over earlier automatic or manual log review systems.

Auditing and Log Management Practices Inhibits Effective Implementation

IT and control system administrators no longer have to manage logs using unwieldy or homegrown, unchecked management scripts and rudimentary reporting templates. New log management and analysis tools have a wide range of features to ease the pain of event logging and incident detection. They can integrate multiple log formats from widely distributed sources and most provide support for automating log collection if it isn't being done already. Event logs from most devices and applications—even legacy systems-can be collected remotely and automatically.

The updated analysis engines available in the log management tools also speed data processing and formatting, making it cheaper and easier to review the functional, operational, and security data. In addition, today's log management systems provide an unprecedented level of ability to select necessary events as

required for compliance reporting, root cause failure analysis, and incident detection.

Event Auditing and Log Management Resources

ICS-CERT has identified a short list of resources for improving event auditing and log management. This resource list is a starting point for learning about log management and is not intended to be comprehensive.

Policies and Recommended Practices

- "Guide to Computer Security Log Management," NIST
- "Information System Audit Logging Requirements," SANS
- "Log Review and Management," OWASP
- "A Practical Application of SIM/SEM/SIEM Automating Threat Identification," SANS
- Security audit policy template, SANS_

Security Policy for Operating Systems

- "Advanced Security Audit Policy Step-by-Step Guide," Microsoft
- "Implementing SCADA Security Policies via Security-Enhanced Linux," Ryan Bradetich and Paul Oman

ROLE OF FUSION CENTERS

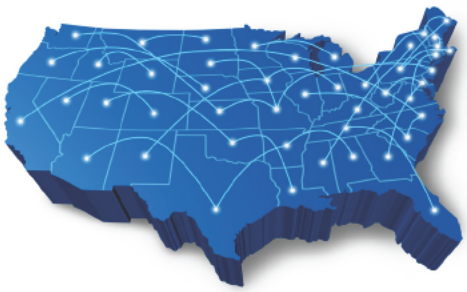
State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT), and private sector partners. Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities. Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

There are currently 77 fusion centers located across the country. These fusion centers are owned and operated by state and local entities and receive support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding. The DHS Office of Intelligence and Analysis (I&A) leads federal coordination and support for fusion centers and has deployed over 95 personnel, including Intelligence Officers, Regional Directors, Reports Officers, and Intelligence Analysts to support fusion centers and to improve the two-way flow of information between fusion centers and the federal government. I&A has also worked aggressively to deploy Homeland Secure Data Network (HSDN) to over 60 fusion centers. HSDN provides SECRET-level connectivity to enhance the ability of state and local partners to receive federally generated classified threat information.

By building trusted relationships and collaborating with SLTT and private sector partners, fusion centers can gather and share the information necessary to pursue and disrupt activities that may be indicators of, or potential precursors to, terrorist activity. With timely, accurate information on potential terrorist threats, fusion centers can directly contribute to and inform investigations initiated and conducted by federal entities, such as the Joint Terrorism Task Forces led by the Federal Bureau of Investigation. According to the 2010 National Security Strategy, the federal government must continue to integrate and leverage fusion centers to enlist all of our intelligence, law enforcement, and homeland security capabilities to prevent acts of terrorism on American soil. Efforts to protect the homeland require the timely gathering, analysis, and sharing of threat-related information. Fusion centers provide a mechanism through which the federal government, SLTT, and private sector partners come together to accomplish this purpose.

For private sector partners working in critical infrastructure, fusion centers offer a local interface for reporting and receiving analytical information on threats relating to their local areas and industries. Many fusion centers can provide information relating to physical and cyber threats that impact local industries and can support efforts to develop and improve local situational awareness, which can in turn improve private sector security planning.

To find a fusion center closest to you, visit the DHS Fusion Center Locations and Contact Information website. ICS-CERT recommends that asset owners and operators contact their local fusion center to get acquainted and to better understand the role of their fusion center in supporting the private sector in critical infrastructure protection and cybersecurity. Asset owners and operators may contact the ICS-CERT directly or work through their fusion centers to contact the ICS-CERT for assistance in mitigating cyber incidents relating to industrial control systems.

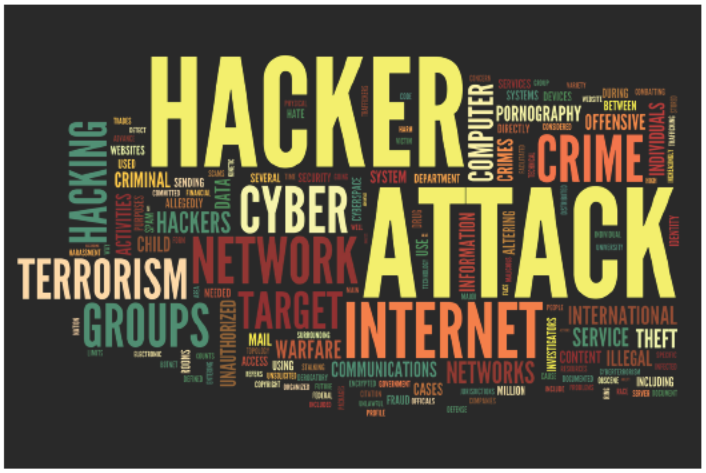


WHAT DOES A CYBER ATTACK FEEL LIKE? TAKE THE CSSP "ICS ADVANCED TRAINING" COURSE AND FIND OUT.

It is two o'clock in the afternoon, and suddenly a tank begins to overflow. Your equipment monitoring instrumentation displays normal operating parameters, and no alarms have triggered in your system. You assume manual control of the process and attempt to restore the process to a safe state.

What just happened? Why didn't an alarm register? Why are your instruments reading normal? What is your next step?

Most enterprises would consider themselves lucky not to have experienced a cyber attack against their control system. Attacks against production systems are extremely undesirable; however, the insight gained as a result of the experience can be valuable and can be used in the event of an attack on real-world industrial control assets.



The Control Systems Security Program (CSSP) provides ICS Advanced Cybersecurity Training, which is a 5 day, hands on training session that affords this insightful experience. The course focuses on ICS protection by presenting specific defensive and offensive tools and techniques. Attacks on ICS are demonstrated in a classroom environment and participants are given the chance to nefariously manipulate actual ICS hardware and software. They do not just discuss these exploits, but actively manipulate and deploy them on actual systems.

Fortunately, the result of mixing the green and yellow liquids causes only the creation of a blue liquid, not a hazardous or otherwise dangerous substance. However, the implications of a comparable attack against real-world industrial processes can certainly be realized by those participating in this training.

The ICS Advanced Cybersecurity training offers step-by-step guidance throughout several topics, including: network discovery, exploitation, defense, and detection. After the 3 full days of classroom instruction are completed, participants are armed with an arsenal of cyber attack and defense tools and techniques. The participants are divided into two teams, red (attackers) and blue (defenders). On the following day, those teams face off in a 12-hour Red Team/Blue Team exercise, and the fun begins.

Once the red and blue identification lanyards are distributed, the participants assume the assigned roles of attackers and defenders. The person sitting next to you in the classroom could now be an adversary, and the mental games and social engineering begins immediately. The blue team is cautioned to guard their sensitive network diagrams, even later that evening at their hotel.

The blue team becomes familiar with their facility, and the red team prepares to bring a forceful attack to disrupt the blue team's critical process. They also target intellectual property that could provide economic advantage against the rival company.

The day is long and intense as attacks are executed by the red team. The blue team moves to detect, defend, and install software mitigations that would prevent new attacks via the same vector. The critical process controlled by the blue team cannot be disrupted without senior management approval, maintaining the realism found in a real-world industrial environment.

On the final day, the exercise is reviewed from both teams' perspectives. As a group, they discuss what happened versus what was perceived to be happening, which techniques were successful for each team, and what could have been done better on each side.

This training session takes place on a monthly basis and is free to attend. For a full schedule of CSSP events, including training, see the CSSP Calendar. Currently, four training sessions are scheduled:

If you would like to learn more about training opportunities, please contact cssp_training@hq.dhs.gov.

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-12-046-01 - Increasing Threat to Industrial Control Systems"

Alert "ICS-ALERT-12-020-05A - KOYO ECOM100 Multiple Vulnerabilities"

Alert "ICS-Alert-12-020-02A - Rockwell Automation ControlLogix Multiple PLC Vulnerabilities"

Alert "ICS-ALERT-12-020-03A - Schneider Electric Modicon Quantum Multiple Vulnerabilities"

Alert "ICS-ALERT-12-039-01 - Advantec Broadwin RPC Server Vulnerability"

Alert "ICS-ALERT-12-034-01 - SSH Scanning Activity Targets Control Systems"

ADVISORIES

Advisory "ICSA-12-058-01 - ABB Robot Communications Runtime Buffer Overflow Vulnerability"

Advisory "ICSA-12-025-02A - 7T TERMIS"

Advisory "ICSA-12-025-02 - 7T Termis DLL Hijacking"

Advisory "ICSA-12-047-01A - Advantech WebAccess Multiple Vulnerabilities"

Advisory "ICSA-12-025-01 - 7T Aquis DLL Hijacking"

Advisory "ICSA-12-025-02 - 7T Termis DLL Hijacking"

Advisory "ICSA-12-047-01A - Advantech WebAccess Multiple Vulnerabilities"

Advisory "ICSA-12-025-01 - 7T Aquis DLL Hijacking"

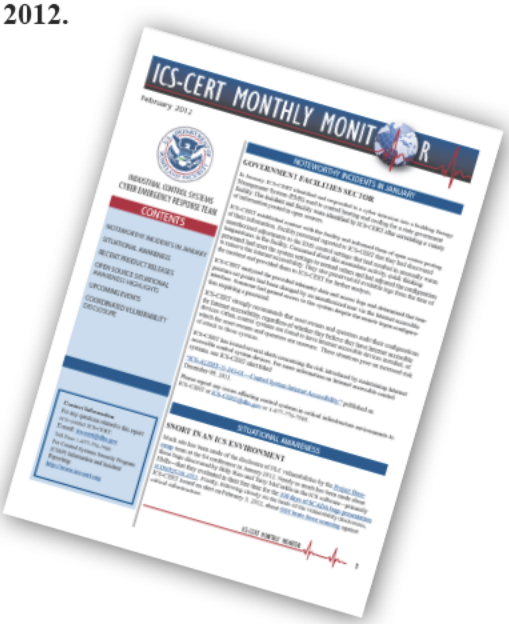
Advisory "ICSA-12-047-01 - Advantech WebAccess Multiple Vulnerabilities"

Advisory "ICSA-12-039-01- Invensys Wonderware HMI Reports XSS and Write Access Violation Vulnerabilities"

Advisory "ICSA-12-013-01 - ING. Punzenberger COPA-DATA GMBH DoS Vulnerabilities"

Other

The ICS-CERT Monthly Monitor February 2012 issue includes highlights of activities from January 2012.



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.

Lawmakers fear power grid could fall to cyber attack
2012-02-28
Many electrical networks now operate on "smart grid" technology, which relies on computers to determine electrical needs. The technology is more energy efficient, but makes the systems vulnerable to cyber attacks.
http://thehill.com/blogs/hillicon-valley/technology/213015

NIST issues new WiFi security guidelines
2012-02-27
The growth of mobile devices across the government is causing agencies to look twice at how they can secure their internal WiFi networks.
http://www.federalnewsradio.com/?nid=246&sid=2763280
http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

GPS jammers and spoofers threaten infrastructure, say researchers
2012-02-23
During the GNSS Vulnerability 2012 event at the UK's National Physical Laboratory on Wednesday, experts discussed the threat posed by a growing number of GPS jamming and spoofing devices. The increasing popularity of the jammers is troubling, according to conference organizer Bob Cockshott, because even low-power GPS jammers pose a significant threat to cell phone systems, parts of the electrical grid, and the safety of drivers.
http://arstechnica.com/business/news/2012/02/uk-research-measures-growing-gps-jamming-threat.ars

Iran Claims Stuxnet Infected 16,000 Computers
2012-02-22
Stuxnet has gained notoriety as the first cyber weapon reported to be deployed with impressive results. Thousands of Iran's nuclear centrifuges were apparently destroyed by the computer virus. Now Iran is telling its side of the story.
http://theinfoboom.com/articles/iran-claims-stuxnet-infected-16000-computers/

NSA Reportedly Concerned About Anonymous Power Grid Attack
2012-02-21
The National Security Agency (NSA) is apparently concerned that Anonymous will try to take down the nation's electrical grid via a cyberattack, according to a new report.
Anonymous, however, says the claims are just fear-mongering.
http://www.pcmag.com/article2/0,2817,2400493,00.asp

http://online.wsj.com/article_email/B10001424052970204059804577229390105521090-lMyQjAxMTAyMDIwMDEyNDAyWj.html

http://gcn.com/articles/2012/02/21/anonymous-nsa-power-grid-friday-attacks.aspx

http://www.isssource.com/hacktivists-could-bring-down-grid/

Digital Bond gives Valentine of critical infrastructure exploit tools
2012-02-15
Digital Bond, a group of researchers dedicated to exposing information security flaws in industrial control systems, released on Valentine's Day a number of exploits of programmable logic controllers (PLCs) that regulate critical infrastructure processes.
http://www.infosecurity-magazine.com/view/23945/

Senators Unveil Major Cybersecurity Bill
2012-02-14
The legislation would codify some of the authority the Obama administration has granted the Department of Homeland Security over federal civilian agency IT security and create the National Center for Cybersecurity and Communications within DHS, headed by a Senate-confirmed director, to coordinate federal efforts to battle cybersecurity threats facing the government and the nation's critical information infrastructure, the mostly privately owned networks that control the flow of money, energy, food, transportation and other vital resources that the economy needs to function.
http://www.govinfosecurity.com/articles.php?art_id=4506

US energy systems have disaster written all over them
2012-02-10
The U.S. power industry, with the support of the government, is engaged in a massive effort to upgrade the nation's power grid from a 19th-century infrastructure to a smart system that takes advantage of and is capable of supporting 21st-century technology. It is a big job, but technologically it is fairly straightforward. We create a standards-based, interoperable network that is capable of two-way transmission of power and data. The challenges are twofold: How do we take advantage of this smart grid infrastructure to reduce our dependence on traditional fossil fuel, and how do we secure it?
http://gcn.com/articles/2012/02/13/cybereye-us-energy-systems-smart-grid.aspx

New Tool Will Automate Password Cracks on Common SCADA Product
2012-02-08
The fallout from last month's S4 Conference continues in February, with a planned Valentine's Day release of tools that make it easy to test and exploit vulnerable programmable logic controllers and other industrial control systems. Among the releases will be a tool for cracking passwords on the common ECOM programmable logic controllers by Koyo Electronics, a Japanese firm, according to a blog post by Reid Wightman for Digital Bond.

Writing on Wednesday, Wightman said that a Valentine's Day release would include a 'module to brute-force' passwords for Koyo's ECOM and ECOM100 PLCs. Researchers revealed that those devices have limited password space (forcing customers to implement short, weak passwords) and, even worse, no lockout or timeout feature to prevent multiple login attempts used in brute force attacks.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

http://threatpost.com/en_us/blogs/new-tool-will-automate-password-cracks-common-scada-product-020812

Utilities Facing Brute-Force Attack Threat
2012-02-06
SSH attack warning from ICS-CERT just the latest in a series of high-profile vulnerabilities in '1990s-era security' SCADA, critical infrastructure world.
http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232600345/

State of SCADA Security Worries Researchers
2012-02-05
Researchers examined the state of security in SCADA and industrial control systems and presented an ugly picture of the vulnerabilities and challenges in addressing the issues.
http://www.eweek.com/c/a/Security/State-of-SCADA-Security-Worry-Researchers-234517/

The Sherpa: Basecamp Redux
2012-02-01
I've experienced a lot of cognitive dissonance concerning the Basecamp disclosure and exploit tools release over the last few months. I might as well explain some more thinking of why doing what we've done is a good idea in the end.
http://www.digitalbond.com/2012/02/01/the-sherpa-base-camp-redux/

Use Purchasing Decisions to Demand Better ICS Security
2012-02-01
It's time we got more vocal and named and shamed indifferent vendors on a regular basis. Plus, we should consider how much assistance a vendor will provide in helping us maintain good security and factor this into our purchasing scorecards.

Nowadays the issue of governance matters to us as professionals and to the Board of Directors of the organizations we work for. Boards have a legal and fiduciary duty to the company and to shareholders to know what's going on and to protect assets and their value. They won't want the details, but if you can explain a purchasing choice by saying "this vendor enables me to enforce your policies and the losing bidders don't" then you shouldn't have many problems.
http://www.tofinosecurity.com/blog/use-purchasing-decisions-demand-better-ics-security

Cyber Attacks Becoming Top Terror Threat, FBI Says
2012-02-01
Cyber attacks against government agencies and businesses in the United States continue to rise, and cyber threats will one day surpass the danger of terrorism to the United States, intelligence community officials said in an open hearing of the Senate select intelligence community Tuesday.

"Stopping terrorists is the number one priority," said FBI director Robert Mueller. "But down the road, the cyber threat will be the number one threat to the country. I do not think today it is necessarily [the] number one threat, but it will be tomorrow."
http://www.informationweek.com/news/government/security/232600046

CYBER TIPS

For processes requiring extended certification run-in testing prior to release for operations, make either virtual copies of the tested configuration or a pair of duplicate hard drives for each station. In the event of system upset or intrusion, the first set can be swapped in, and the original hard drives removed for forensics. If the first replacement images or drives get quickly corrupted, the asset owner is given one more chance to resolve the infection and still have one last certified set of images or drives to allow quick restoration to the last operational configuration.

We Want to Hear from You

A key aspect of our mission is providing relevent and timely cybersecurity information products and services to ICS stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we cn 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.

UPCOMING EVENTS

APRIL

Energy & Power Cyber Security Summit
April 04–06, 2012
Sheraton Atlanta Hotel
Atlanta, Georgia
Contact info: Timothy Downs, tdowns@interworkmedia.com, http://www.energysecuritysummit.com/
949-766-6785

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (1 week)
April 9-13, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

MAY

ICSJWG Spring Conference
May 7–10, 2012
Hyatt Regency Savannah
Savannah, Georgia
Conference Information
Registration

ICSJWG Conference Training Introductory Training: Introduction to Control Systems Cybersecurity (Course 101, 8 Hours)
May 10, 2012
Hyatt Regency Savannah
Savannah, Georgia
Course Description
Registration

International Community Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop **(1 week)**
May 14-18, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

NESCO Town Hall Security Risk Management Practice for Electrical Utilities
May 30–31, 2012
New Orleans Marriott
New Orleans, Louisiana
Contact Info: Abbie Trimble, abbie@energysec.org
http://nescotownhall2012.eventbrite.com/

NERC CIP Compliance Training
May 24–10, 2012
Newark Liberty International Airport Marriott
Newark, New Jersey
Contact Info: Abbie Trimble, abbie@energysec.org,
http://cipcompliance-newark.eventbrite.com/

JUNE

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (1 week)
June 18-22, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

JULY

NERC CIP Compliance Training
July 12, 2012
Minneapolis Airport Marriott
Minneapolis, Minnesota
Contact Info: Abbie Trimble, abbie@energysec.org,
http://cipcompliance-minneapolis.eventbrite.com/

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (1 week)
July 16–20, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

OCTOBER

NERC CIP Compliance Training
October 25, 2012
SpringHill Suites, Las Vegas Convention Center
Las Vegas, Nevada
Contact Info: Abbie Trimble, abbie@energysec.org,
http://cipcompliance-lasvegas.eventbrite.com/

DOCUMENT FAQ

What is the publication schedule for this digest?

ICS-CERT publishes the "ICS-CERT Monthly Monitor" approximately 12 times per year. Generally, 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

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. 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.

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. This coordinated disclosure process ideally allows time for a vendor to develop and release patches and for users to test and deploy patches prior to public disclosure of the vulnerability. While this process is not always followed for a variety of reasons, ICS-CERT continues to strive for this as a desirable goal.

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 Researchers in February 2012.

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

- Luigi Auriemma, coordinated via ZDI, ICSA-12-058-01 - ABB Robot Communications Runtime Buffer Overflow Vulnerability, February 28, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-025-02 - 7T TERMIS DLL Hijacking, February 17, 2012.
- The nSense Vulnerability Coordination Team, Greg MacManus of iSIGHT Partners, Kuang-Chun Hung of Security Research and Service InstituteInformation and Communication Security Technology Center (ICST), Luigi Auriemma, Billy Rios, Terry McCorkle, and Snake (alias) separately reported to ICS-CERT, ICSA-12-047-01A – Advantech WebAccess Multiple Vulnerabilities, February 17, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-025-01 - 7T AQUIS DLL Hijacking, February 17, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-047-02 - Advantech WebAccess Multiple Vulnerabilities, February 16, 2012.
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-013-01 - ING. Punzenberger COPA-DATA GMBH DoS Vulnerabilities, February 07, 2012.
- Billy Rios and Terry McCorkle, ICSA-12-039-01 - Invensys Wonderware HMI Reports XSS and Write Access Violation Vulnerabilities, February 08, 2012.

Researchers Currently Working with ICS-CERT this fiscal year.

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Luigi Auriemma	Joel Langill	Rubén Santamarta	Dillon Beresford	Eireann Leverett
Secunia	Yun Ting Lo (ICST)	Kuang-Chun Hung (ICST)	Terry McCorkle	Shawn Merdinger
Celil Unuver	Knud Erik Højgaard (nSense)	Billy Rios	Greg MacManus (iSIGHT Partners)	
Carlos Mario Penagos Hollmann				