ICS-CERT MONTHLY MONITOR

May 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

INCIDENT RESPONSE ACTIVITY IN APRIL

SITUATIONAL AWARENESS

CSSP NEWS

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy

Contact Information

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

Email: ics-cert@hq.dhs.gov

Toll Free: 1-877-776-7585

For Control Systems Security Program (CSSP) Information and Incident Reporting:

http://www.ics-cert.org

INCIDENT RESPONSE ACTIVITY IN APRIL

REMOVABLE MEDIA FLASH DRIVE INFECTION

In April, an energy company experienced a near miss incident related to a potential malware infection in its control system. A shift supervisor was downloading information from the human-machine interface (HMI) connected to the industrial control systems (ICSs) onto a portable removable media flash drive as part of his normal duties. At the end of the shift, the supervisor mistakenly left the removable media in the USB port of the HMI computer. Later, other workers discovered the removable flash drive in the HMI, immediately removed it, and began an investigation. They ran antivirus scanners on the removable media, the HMI machine, and other associated systems. The antivirus scanners found the Hamweq virus on the removable media, but the other systems were clean.

The malware did not infect the HMI or the associated ICS because the auto-run function had been disabled on their systems. If auto-run had been enabled, the malware could have injected malicious code to the connected systems and created a backdoor through remote Port 6667/TCP. No malicious intent was attributed to the supervisor. The critical error precursors that led to this incident were:

- removable media flash drives not properly marked,
- removable media flash drives that have been deemed unusable not properly segregated, and
- a personally owned removable media drive used in systems associated with ICS.

The following recommended practices concerning removable media can help to prevent infections on critical systems:

- Never insert removable media with an unknown origin into a system.
- Never mix personally owned removable media with company-owned removable media.
- Always use dedicated media for the same systems.
- Always clearly label removable media.
- Always segregate malfunctioning or suspected infected removable media from media that is deemed acceptable.
- Disable the auto-run function on ICS when practical.

Combating sophisticated attacks is challenging for any company. ICS-CERT is working with partners to evaluate a more strategic and layered approach to detecting and mitigating these threats. ICS-CERT continues to recommend Defense-in-Depth practices and to educate users about social engineering and spear-phishing attacks. Organizations are also encouraged to review ICS-CERT's Incident Handling Brochure for tips on preparing for and responding to an incident.

MANAGING THE COMPLEXITIES OF VULNERABILITY DISCLOSURE IN AN INTERNATIONAL ENVIRONMENT

On any given day, ICS-CERT responds to requests for information from other government agencies and private sector industry groups and personnel. ICS-CERT also manages the vulnerability disclosure process—both coordinated and unanticipated—from start to finish, as well as generating alerts and advisories that address the ICS threat environment.

The international nature of the work often determines the role played by ICS-CERT in the vulnerability disclosure process. International law regarding security research, regulatory requirements, and intellectual property plays a part in determining the ICS-CERT relationship with vendors, security teams, and researchers. Managing communications across multiple organizations operating in multiple time zones and different languages similarly influences how ICS security threats are identified and addressed. Another key factor in the response process stems from differences in international software vulnerability commercialization.

Two examples of the internationalization of ICS-CERT efforts are provided here to highlight the importance of ICS security and critical infrastructure protection in the global security arena. These examples also demonstrate how this internationalization has affected vulnerability disclosure and incident response regarding ICS security threats.

Logistics of International Communications

During the security update development process, ICS-CERT maintains routinely scheduled communication with both the vendor and the researcher. In some cases, as with the 100 Bugs in 100 Days: An Analysis of ICS (SCADA) Software, the team managed the disclosure of vulnerabilities discovered by researchers Billy Rios and Terry McCorkle. As if tracking that many bugs wasn't difficult enough, the researchers and ICS-CERT also had to coordinate resolution of the vulnerabilities with multiple ICS vendors.

ICS-CERT coordinated vendor response and advisory publication across multiple countries, time zones, languages, and communications formats. Simply coordinating emails and phone calls between the vendors and researchers required months of dedicated effort by everyone involved.

International Security Markets

Response to ICS-CERT vulnerability disclosure management efforts range widely, dependent on the location of the researcher, the security team, the vendor, or the country-specific CERT involved. In addition, the approach that researchers take to disclosing vulnerabilities varies greatly.

The means by which researchers disclose information regarding security-impacting software flaws directly influences how the ICS-CERT and other CERT organizations manage relationships with the researchers.

These market differences require ICS-CERT to take a much more flexible approach to coordination and vulnerability disclosure management when dealing with non-U.S. researchers. These differences could also limit the level of engagement between ICS-CERT and foreign researchers, subsequently impacting ICS-CERT's ability to mitigate threats.

XP END OF LIFE

Extended support for the Microsoft Windows XP Service Pack 3 is scheduled to end on April 8, 2014, according to the Windows Lifecycle Fact Sheet released by Microsoft. Impacted organizations have only 12 months to decide whether to migrate their XP SP3 systems or to plan on upgrading them to a supported Windows operating system.

Areas of Concern for Industrial Control Systems

- Industrial control system vendors and integrators, however, do not always incorporate Windows life cycle support into their ICS development life cycle and support plans. ICS-CERT has identified three technology deployment areas ICS teams should evaluate when considering how to address the upcoming EOL of XP SP3 across ICS environments. ICS applications installed on Windows XP SP3 operating system builds on standard IT equipment, including engineering workstations, HMI servers, historian systems, etc.
- ICS applications that require a specific Microsoft browser version that may no longer be supported or available except as part of an XP SP3 installation.
- ICS devices with embedded XP or Windows CE operating systems such as PLCs or RTUs.

Understanding the Windows Support Life Cycle

ICS support teams, vendors, and integrators need to understand the Microsoft Support Lifecycle and how it impacts application life-cycle management or system administrative support. By understanding the product support available, customers can better maximize the management of IT investments and make strategic plans for future IT needs.

New operating systems are adopted more slowly by ICS vendors and integrators than even the most risk-averse IT teams, because the ICS vendors must update their software for deployment on the new platform, identify any potential area of availability or integrity concerns, and resolve any functional or stability issues that may arise.

SITUATIONAL AWARENESS (Continued)

What Extended Support Entails

Extended support, the phase in which XP SP3 currently resides, is the second portion of the Windows Product Support Lifecycle. The key differences between mainstream and extended support are that the free support options are no longer available and that Microsoft no longer provides new, nonsecurity hotfixes.

Product End of Life

Because XP SP3 is scheduled to move into end of life in April 2014, anyone using or providing software dependent on the platform should begin planning to move to a supported operating system as soon as possible.

CSSP NEWS

ICSJWG 2012 SPRING CONFERENCE

The Industrial Control Systems (ICS) Joint Working Group (JWG) recently held the ICSJWG 2012 Spring Conference in Savannah, Georgia. The conference consisted of panel discussions, presentations, and training on various topics such as incident response, responsible disclosure, standards development, threat and incident reporting, analysis tools and techniques, roadmap development initiatives, vulnerability management, research and development, and information sharing.

Incident response emerged as a common theme at the conference. The conference kicked off with a plenary session presented by Eric Cornelius from DHS and FBI Special Agent Christopher Trifiletti. Their presentation discussed the highly publicized incident at Curran-Gardner Water District in Springfield, Illinois. The presentation was well attended and generated significant interest. Attendees gained an insight into the resources and information the FBI and ICS-CERT used to disprove the occurrence of a cyber attack. In another session, ICS-CERT's Kevin Hemsley presented a report on ICS-CERT's past and present incident response activities. He noted that in total, ICS-CERT has handled over 300 incidents since late 2009. Attendees also learned how ICS-CERT provides incident response remotely, and discussed the details of 17 separate incidents where ICS-CERT provided onsite assistance to asset owners. Another topic was the ability of ICS-CERT to leverage information obtained from response activities to provide situational awareness warnings and alerts to the rest of the CIKR community and NCCIC partners. ICS-CERT provides guidance for impacted organizations and recommends a path for recovery and future protection; however, ICS-CERT does not provide direct recovery services for impacted organizations.

Other notable events at the ICSJWG included:

- Subgroup Meetings: The subgroup meetings were held on the first day of the conference and allowed participants to discuss in depth the current status of subgroup activities and report accomplishments to the community.
- Cybersecurity Training: An 8-hour Introduction to Control Systems Cybersecurity training course was taught to some 150 conference attendees. This course introduces students to the basics of industrial control systems security. The class included a comparative analysis of IT and control system architecture, security vulnerabilities, and mitigation strategies unique to the control system domain.
- International Partners' Day: A day of information sharing sessions provided by various international organizations that attended. Attendees had the opportunity to discuss goals, milestones, and the path forward for possibly creating a new ICSJWG subgroup. In May, several of the international attendees to Spring ICSJWG Conference also attended the world-renowned, "hands-on" Industrial Control Systems (ICS) Cybersecurity Advanced Training held in Idaho Falls, Idaho.

The ICSJWG Fall Conference will be held October 15–18, 2012, in Denver, Colorado. The Fall Conference is open to all who are interested in learning more about cybersecurity issues facing critical infrastructure control systems. For more information on past and future ICSJWG conferences, visit the website at http://www.us-cert.gov/control_systems/icsjwg/ or email icsjwg@dhs.gov.

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-12-116-01A—(UPDATED) RuggedCom Weak Cryptography for Password Vulnerability

ICS-ALERT-12-116-01—RuggedCom Weak Cryptography for Password Vulnerability

ICS-ALERT-12-020-03B—(UPDATED) Schneider Electric Modicon Quantum Multiple Vulnerabilities

ICS-ALERT-12-019-01A—(UPDATED) GE D20ME PLC Multiple Vulnerabilities

ICS-ALERT-12-097-02—3S-Software Codesys Improper Access Control

ICS-ALERT-12-097-01—WAGO IPC Multiple Vulnerabilities

We Want to Hear from You

A key aspect of our mission is providing relevent and timely cybersecurity information products and services to industrial control system (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 can 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@hq.dhs.gov.

ADVISORIES

ICSA-12-030-01A—Siemens SIMATIC WinCC Multiple Vulnerabilities

ICSA-12-102-01—Certec WebMI2ADS Multiple Vulnerabilities

ICSA-12-102-02—Koyo ECOM Modules Multiple Vulnerabilities

ICSA-12-102-03—Microsys Promotic Use After Free Vulnerability

ICSA-12-102-04—Siemens Scalance X Buffer Overflow Vulnerabilities

ICSA-12-102-05—Siemens Scalance S Multiple Security Vulnerabilities

ICSA-12-095-01A—(UPDATED) ABB Multiple Platform Components Buffer Overflow

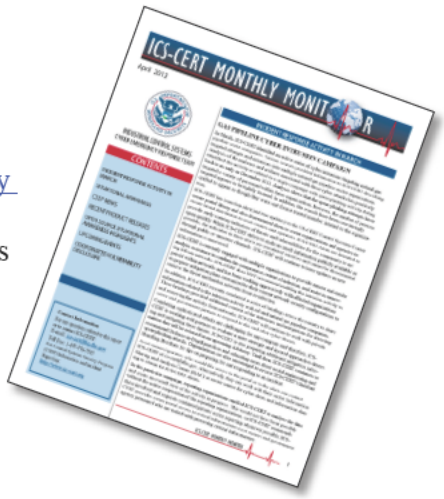
ICSA-12-088-01A—Rockwell Automation FactoryTalk RNADiagReceiver

ICSA-12-095-01—ABB Multiple Platform Buffer Overflow

ICSA-12-062-01—Invensys Wonderware Information Server Multiple Vulnerabilities

OTHER

The ICS-CERT Monthly Monitor April 2012 issue includes highlights of activities from March 2012.



OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

ICS-CERT compiles this section from multiple resources including current events as disclosed on Web sites, 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.

'Bullet time' to stop cyber attacks on power grids

2012-04-30

The idea, from security engineers at the University of Tulsa in Oklahoma, is to slow down internet traffic, including malicious data, to give networks time to deal with attacks. To do this, when a cyber attack has been sensed, an algorithm sends hyper-speed signals accelerating ahead of the malicious data packets to mobilize defenses.

Such measures are needed because cybercriminals increasingly seem to target crucial industrial infrastructure. In 2010, for example, the Stuxnet worm infected Iran's nuclear program. It was shown to be not so much a typical computer virus as a multifunctional weapon that can be reprogrammed to target any crucial industry. As industrial systems generally go for many years without software upgrades or password changes, they can often be vulnerable to such attacks.

http://www.newscientist.com/article/dn21756-bullet-time-to-stop-cyber-attacks-on-power-grids.html

The real threat: China, Iran or our own weaknesses?

2012-04-27

That such an attack has not happened yet does not mean it cannot happen, today or tomorrow or sometime in the not-too-distant future. But whatever the level of current risk, it is important that the U.S. use the time available to prepare and defend its systems. The government has a legitimate interest in ensuring that this happens and providing assistance where needed, and this inevitably will involve legislation and mandated standards of security.

It is important that these mandates go beyond checklist baselines of security controls, however, and embrace a comprehensive life-cycle approach for the critical infrastructure that will enable effective security based on risk management.

http://gcn.com/articles/2012/04/27/cybereye-lack-of-fundamentals-threat-to-security.aspx

Backdoor in mission-critical hardware threatens power, traffic-control systems

2012-04-25

In the world of computer systems used to flip switches, open valves, and control other equipment inside giant electrical substations and railroad communications systems, you'd think the networking gear would be locked down tightly to prevent tampering by vandals. But for customers of Ontario, Canada-based RuggedCom, there's a good chance those Internet-connected devices have backdoors that make unauthorized access a point-and-click exercise.

http://arstechnica.com/business/news/2012/04/backdoor-in-mission-critical-hardware-threatens-power-traffic-control-systems.ars

Security pros not ready for attacks, still don't want government regs

2012-04-25

Security professionals believe cyberattacks are coming, but they aren't sure what to do about them and don't want government involved in protecting them, according to a recent survey by security company Bit9.

Two-thirds of those surveyed believe they will be the targets of cyberattacks in the next six months, and most say their current security is inadequate but they do not think government regulation will improve it. Implementing best practices and better security policies is the best way to improve security, most said. But left to their own devices, they have not yet done this.

http://gcn.com/articles/2012/04/25/bit9-cybersecurity-survey-expect-attacks-but-no-regulations.aspx
http://www.bit9.com/files/Research_Bit9_US_Global_Survey_2012_FINAL.pdf
http://grassrootslinux.com/cybersecurity-bills-cannot-fix-our-problems/

Major cyberattack on US 'inevitable,' experts tell Congress

2012-04-24

A panel of cybersecurity professionals warned lawmakers that voluntary guidelines for securing the nation's critical infrastructure have not worked and that Congress must pass strong cybersecurity legislation that sets basic security standards in order to avoid a damaging cyberattack.

http://gcn.com/Articles/2012/04/24/Cyber-security-hearing-major-attack-inevitable.aspx

Suspected cyber attack hits Iran oil industry

2012-04-23

Iran is investigating a suspected cyber attack on its main oil export terminal and on the Oil Ministry itself, Iranian industry sources said on Monday.

A virus was detected inside the control systems of Kharg Island - which handles the vast majority of Iran's crude oil exports- but the terminal remained operational, a source at the National Iranian Oil Company (NIOC) said.

http://www.reuters.com/article/2012/04/23/net-us-iran-oil-cyber-idUS-BRE83M0P120120423

Control System Security Center Against Cyber-Attacks Established in Japan

2012-04-20

An assembly of about 60 representatives from industrial companies, research institutes and industrial associations, along with representatives from the Ministry of Economy, Trade and Industry (METI), gathered for the first general meeting of The Research & Development Partnership Control System Security Center, held in Tokyo on April 16, 2012.

http://www.arcweb.com/industry-news/2012-04-20/control-system-security-center-against-cyber-attacks-established-in-japan.aspx

Wearable Firewall Stops Pacemaker Hacking

2012-04-19

Millions of people use insulin pumps, pacemakers and other personal medical devices that rely on wireless communication to function. But what happens if someone was to tamper with that vital communication line between the health care provider and the patient?

http://www.securitynewsdaily.com/1753-firewall-prevent-pacemaker-hacking.html

Smart grid cybersecurity not keeping pace with deployment, survey finds

2012-04-18

Three-quarters of energy security professionals believe cybersecurity has not been adequately addressed in smart grid deployment, according to a survey by EnergySec and nCircle.

http://www.infosecurity-magazine.com/view/25245/smart-grid-cybersecurity-not-keeping-pace-with-deployment-survey-finds/

How Did They Get In? A Guide To Tracking Down The Source Of An APT

2012-04-18

Advanced persistent threats are a complex security problem, but there are two things that all APTs have in common: They are hard to detect and come into your network in unusual (often zero-day) ways. it is difficult to uncover an APT, but, once you do, the hard work really begins: finding the source of the problem, identifying the attacker and figuring out to what extent the attack has affected your organization's systems.

Discovering the actual APT attack code requires a proactive, hands-on approach involving in-depth analysis of log files, network traffic and program code. The goal is to uncover behavior indicative of APT activity: network exploration and data exfiltration. Even the best and brightest security teams may be challenged by the sophistication of some of the attacks we have seen lately, but security professionals should at least have an understanding of the methods used to carry out an APT.

http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232900475/

DOE Lab Releases Open-Source Attack Intelligence Tool

2012-04-17

The U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL) is offering an open-source version of a home-grown tool that gathers an additional layer of intelligence during an attack.

The so-called Hone tool is basically a host-based sensor that automatically pinpoints which applications or processes infected machines and an external network they are using to communicate. So it could help determine the specific app used between a bot and its command-and-control, or between an infected machine and the attacker trying to siphon information or intellectual property.

http://www.darkreading.com/advanced-threats/167901091/security/application-security/232900471/

https://github.com/HoneProject

ABB Refuses to Patch Vulnerabilities in Legacy Systems

2012-04-05

Researchers Terry McCorke and Billy Rios identified a buffer overflow flaw in a number of components of the ABB WebWare Server applications that are currently being used in many legacy ABB products. However, because they're approaching the end of their life cycle, the company revealed that no patches should be expected.

According to an ICS-CERT advisory, there are still some Industrial Control Systems (ICS) which rely on products such as ABB's WebWare Server SDK, ABB Interlink Module, S4 OPC Server, QuickTeach and RobotStudio Lite.

http://news.softpedia.com/news/ABB-Refuses-to-Patch-Vulnerabilities-in-Legacy-Systems-263008.html

DHS: America's water and power utilities under daily cyber-attack

2012-04-04

America's water and energy utilities face constant cyber-espionage and denial-of-service attacks against industrial-control systems, according to the team of specialists from the U.S. Department of Homeland Security who are called to investigate the worst cyber-related incidents at these utilities.

These ICS-based networks are used to control water, chemical and energy systems, and the emergency response team from DHS ICS-CERT, based at the DHS in Washington, D.C. will fly out to utilities across the country to investigate security incidents they learn about. ICS-CERT typically doesn't name the names of the utilities they try to assist, but this week they did provide a glimpse into how vulnerable America is. In a panel at the GovSec Conference, ICS-CERT's leaders candidly presented a bleak assessment of why America's utilities have a hard time maintaining security, and why it's getting worse.

http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html

http://www.techworld.com.au/article/420612/

Weak passwords render major power supplier vulnerable to hackers, audit finds

2012-04-04

A federal utility in the Pacific Northwest that powers 30 percent of the region, including key military installations, is vulnerable to computer breaches, according to an internal Energy Department audit. But the weaknesses highlighted are typical of many critical government and industry systems, say some cybersecurity experts.

http://www.nextgov.com/nextgov/ng_20120404_8857.php?oref=topnews

UPCOMING EVENTS

June

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

HydroVision International 2012
July 17–20, 2012
Louisville, Kentucky

Chemical Sector Security Summit
July 30–August 01, 2012
Baltimore, Maryland

August

GFIRST
August 19–24, 2012
GFIRST Conference
Atlanta, Georgia

September

American Water Works Association (AWWA) Water Security and Emergency Preparedness Conference & Exposition (WSEPC) 2012
September 9–12, 2012
Hilton St. Louis at the Ballpark
St Louis, Missouri

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop (1 week)
September 10–14, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

5th Annual National Dam Security Forum (in conjunction with the Association of State Dam Safety Officials (ASDSO) Dam Safety 2012
September 16–20, 2012
Colorado Convention Center
Denver, Colorado

3rd Annual Cybersecurity Summit
September 27, 2012
Ronald Reagan Building and International Trade Center
Washington, DC

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@hq.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@hq.dhs.gov *or toll free at 1-877-776-7585.*

Notable Coordinated Disclosure Researchers in April 2012.

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

- Independent security researchers Billy Rios, Terry McCorkle, Shawn Merdinger, and Luigi Auriemma, ICSA-12-030-01A—Siemens SIMATIC WinCC Multiple Vulnerabilities," April 18, 2012.
- Luigi Auriemma, ICSA-12-102-01—Certec WebMI2ADS Multiple Vulnerabilities, April 11, 2012.
- Reid Wightmam's S4 BaseCamp Team, ICSA-12-102-02—Koyo ECOM Modules Multiple Vulnerabilities, April 11, 2012.
- Luigi Auriemma, ICSA-12-102-03—Microsys Promotic Use After Free Vulnerability, April 11, 2012.
- Jürgen Bilberger from Daimler TSS GmbH, ICSA-12-102-04—Siemens Scalance X Buffer Overflow Vulnerabilities, April 11, 2012.
- Adam Hahn and Manimaran Govindarasu, ICSA-12-102-05—Siemens Scalance S Multiple Security Vulnerabilities, April 11, 2012.
- Billy Rios and Terry McCorkle, ICSA-12-095-01A—(UPDATED) ABB Multiple Platform Components Buffer Overflow, April 10, 2012.
- Luigi Auriemma, ICSA-12-088-01A—Rockwell Automation FactoryTalk RNADiagReceiver, April 06, 2012.
- Billy Rios and Terry McCorkle, ICSA-12-095-01—ABB Multiple Platform Buffer Overflow, April 04, 2012.
- Billy Rios and Terry McCorkle, ICSA-12-062-01—Invensys Wonderware Information Server Multiple Vulnerabilities, April 02, 2012.

Researchers Currently Working with ICS-CERT in 2012

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)
Justin W. Clarke
Kuang-Chun Hung (ICST)
Terry McCorkle
Shawn Merdinger
Celil Unuver
Knud Erik Højgaard (nSense)
Billy Rios
Greg MacManus (iSIGHT Partners)
Dan Tentler
Alexandr Polyakov
Carlos Mario Penagos Hollmann
Alexey Sintsov
Adam Hahn
Manimaran Govindarasu
Jürgen Bilberger
Reid Wightman