ICS-CERT MONTHLY MONITOR

September 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

MALICIOUS ACTIVITY

SITUATIONAL AWARENESS

TRAINING UPDATE

ASSESSMENT SUMMARY

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

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

ICS-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

MALICIOUS ACTIVITY

SHAMOON

The Shamoon virus is an information-stealing malware application that also includes a destructive module. Kaspersky Lab, Seculert, and Symantec provided the initial Shamoon reports; Symantec first detected Shamoon on August 16, 2012. While ICS-CERT has not received any confirmed reports of US infections to date, this and other types of malware continue to pose a threat to critical infrastructure organizations.

After the initial infection, Shamoon spreads via network shares to infect additional machines on the network. When it is done collecting information, Shamoon disables the infected systems by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable. Current analysis indicates that Shamoon does not specifically target control systems networks. However, because of its destructive capability, ICS asset owners and operators want to ensure that their control system network defenses are strong enough to prevent Shamoon migrating to the ICS in the event of a business network infection within their organization.

According to Symantec, Shamoon has three primary functional components:

1. Dropper—the main component and source of the original infection. It installs a number of other modules.
2. Reporter—this module is responsible for reporting infection information back to the attacker.
3. Wiper—this module is responsible for the destructive functionality of the malware.

Kaspersky Lab also confirmed that Shamoon included a "kill timer" that triggered the malware to begin the destructive wiper action on a specified date. Subsequent reporting indicates a strong possibility that the Shamoon malware was responsible for the recent disabling of a large segment of the Saudi Aramco business network.

While the actual initial infection vector has yet to be determined, this incident highlights both the risk associated with using removable media, and the potential for "insider" network attacks.

The damage in this case, though limited to the business network, was significant. And a similar destructive attack like this could just as easily have occurred on the control systems networks.

MALICIOUS ACTIVITY

MITIGATION STRATEGIES

The bottom line for ICS asset owners and operators is to avoid having their networks "Shamooned" by this destructive malware. Specifically, organizations should create an emergency action plan and act proactively to decrease their exposure to the threat posed by this malware. Specific mitigations include:

- Encourage users to transfer critical files to network shares, to allow for central backup.
- Execute daily backups of all critical systems.
- Periodically execute an "offline" backup of critical files to removable media.
- Establish emergency communications plans should network resources become unavailable.
- Isolate any critical networks (including operations networks) from business systems.
- Identify critical systems and evaluate the need for having on-hand spares to quickly restore service.
- Ensure antivirus is up to date. There are reports that some variants are not being detected by antivirus; however, updating signatures is still prudent.
- Review and update their policies regarding physical and electronic access to critical networks and systems. Access control policies should discuss the use of removable media; it is particularly important to limit removable media use in any control system environment.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall such as HTTP, FTP, mail, and DNS services.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Place control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT recommends that organizations review the ICS-CERT Joint Security Awareness Report JSAR-12-241-01A—Shamoon/DistTrack Malware and Technical Information Paper ICS-TIP-12-146-01A Cyber Intrusion Mitigation Strategies for high-level strategies that can improve overall visibility of a cyber intrusion and aid in recovery efforts should an incident occur.

ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

We Want To Hear From You

A key aspect of our mission is providing relevant 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.

SITUATIONAL AWARENESS

ICS-CERT BECOMES A CVE NUMBERING AUTHORITY

On June 1, 2012, ICS-CERT was officially commissioned by the MITRE Corporation as a CVE Numbering Authority (CNA). This allows ICS-CERT to directly assign Common Vulnerabilities and Exposures (CVE)
identification numbers to vulnerabilities reported to ICS-CERT.

CVE is the industry standard for vulnerability and exposure naming. CVE identifiers provide a reference used by product end users, vendors, and security practitioners to identify specific vulnerabilities and for data exchange so individual vulnerabilities can be uniquely identified.

CNAs organizations distribute CVE identification numbers to researchers and product vendors for inclusion in public announcements of new vulnerabilities.

ICS-CERT works closely with the MITRE Corporation who manages the CVE Initiative and the CERT Coordination Center (CERT/CC) at Carnegie Mellon University. CERT/CC provided support and assistance to ICS-CERT as this enhanced capability was implemented. Their support was greatly appreciated.

ADVANCES IN SMART GRID DETECT POWER THEFTS, REDUCES RISKS

Power losses on the energy grid can be a major problem in power dispatching and load monitoring. Problems with load monitoring and power dispatching can lead to overloading of equipment and systems that could result in the loss of power distribution.

The recent problems in India highlight the vulnerabilities introduced by power theft and overloading, but India is not the only country that is currently facing grid challenges. Countries like Serbia have recently introduced advanced technologies to help measure power loss to better understand where the losses occur and how to minimize them. Serbia is also employing tools to better predict demand in critical areas of the country. Brazil has been fighting a battle against electric theft by upgrading its grid with meticulous metering. Brazil loses approximately 15 percent of its annual energy production to theft. Effective metering helps to identify the accurate electricity usage and helps to predict current and future demand trends.

With the advances in metering and the global shift to smart meters, the power industry is better able to make real-time assessments through instantaneous data collection. Real-time monitoring through smart meters not only helps to diagnose problems more quickly, but also can be used to quickly detect theft. While advances in metering technology make it harder to steal power, the effort to thwarting the new technology also advances. Two recent presentations at BSides and Black Hat exposed tools that could be used to maliciously alter smart meter functionality for devices currently being deployed in the United States. Other smart meter features could potentially be used to alter HVAC controls (i.e., change the temperature), cut power during emergencies, or control automatic lighting during times when consumption needs to be throttled.

As smart metering and measurement systems become more prevalent within the grid, grid operators' ability to efficiently predict loading and to prevent cascading outages will improve significantly. Smart metering will also help to minimize line losses, increase transmission efficiency, and allow the industry to reduce the financial loss from power theft. For more information on smart meters and their effect on the grid, or for smart meter vulnerability information, readers are encouraged to visit the North American Electric Reliability Corporation (NERC) at http://www.nerc.com/ or the Electric Sector ISAC (ES-ISAC) at esisac@nerc.com.

TRAINING UPDATE

AUGUST TRAINING HIGHLIGHTS

Historically, industrial control systems (ICSs) were isolated from the information highway we know as the Internet. That isolation presented a fairly low risk of unauthorized access to the control system operational domain because in most cases physical access was the only access available.

The merging of the formerly isolated control system domain with the Information Technology (IT) domain made information transfer between the domains much easier. It provided nearly instantaneous access to control system data that previously might have required a collation of many data sources. In addition, the merger provided ICS operators the ability to monitor their control systems from remote locations. However, the positive aspects of better connectivity were overshadowed by the introduction of significant vulnerabilities to control system domains through that improved connectivity.

An important facet of ICS-CERT is the training available to control system owners, operators, and vendors, which raises awareness of ICS vulnerabilities and the possible mitigations. The training sessions also provide a venue to address ICS security concerns, develop additional points of contact, and enhance individual technical capabilities for testing and protecting the ICS environment.

This past August, the ICS training group hosted 61representatives from various military facilities to help them become better acquainted with control system infrastructure protection challenges. Attendees included service personnel from physical security, information assurance, ICS operations, and headquarters areas of responsibility. As a result of the training, a regional Installation Command has implemented an ICS-focused Cross Disciplinary Working Group to address common needs and concerns.

The ICS training group also made two presentations—Introduction to Control Systems Cybersecurity (101); and Intermediate Cybersecurity for Control Systems (201)—at the Government Forum on Incident Response Security Teams (GFIRST) Conference in Atlanta, Georgia, the week of August 19, 2012. Over 1,500 people were registered for the conference.

For more information regarding the DHS ICS-CERT see http://www.us-cert.gov/control_systems/. Select the "Training" and "Calendar" links for details on the various training options that are available and the currently scheduled locations and dates.

ASSESSMENT SUMMARY

ICS-CERT RISK EVALUATIONS

During August, ICS-CERT conducted five onsite assessments across three different sectors, including Energy, Water, and Information Technology. The assessments provided a detailed review of each site's critical infrastructure and interconnectivity to identify gaps in security that could be used by an adversary to gain access to the systems. The ICS-CERT assessment teams performed detailed standards evaluations using NIST 800.82 and NIST 800.53, along with a comprehensive architecture and component evaluation at each location. General findings included interconnectivity to external networks that require defense-in-depth strategies to protect them from cyber attacks. The team also discussed options for mitigation to assist the asset owner toward a more secured system. The program also processed and approved the documentation to support an assessment within the Water Sector scheduled in October.

In support of the partnership with the Inter-agency Task Force (IATF) and ICS-CERT, where joint assessment was conducted focusing on physical and cybersecurity, an encryption procedure was developed to assist the asset owners in securely transmitting their assessment results to the IATF for interdependencies with critical infrastructure, and a statewide analysis based on scenarios. ICS-CERT also completed two detailed assessment reports for a vendor assessment and an architecture review of a new control system center to support critical services and operations within the Transportation Sector.

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-12-234-01A- Key Management Errors in RuggedCom's Rugged Operating System (August 31, 2012)

ICS-ALERT-12-234-01- Key Management Errors in RuggedCom's Rugged Operating System (August 21, 2012)

ICS-ALERT-12-214-01- SpecView Directory Traversal (August 01, 2012).

ADVISORIES

ICSA-12-243-01- GarrettCom – Use of Hard-Coded Password (August 30, 2012)

ICSA-12-228-01- Tridium Niagara Multiple Vulnerabilities (August 14, 2012)

ICSA-12-227-01- Siemens COSMOS database privilege escalation vulnerability (August 14, 2012)

ICSA-12-214-01- Siemens Synco OZW default password (August 01, 2012)

OTHER

The ICS-CERT Monthly Monitor August 2012 issue includes highlights of activities from July 2012.

Follow ICS-CERT on Twitter: @icscert

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.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Cyber attack takes Qatar's RasGas offline
2012-08-30

RasGas, the second largest producer of Qatari LNG after Qatar Petroleum, has been hit with an "unknown virus" which has taken the company offline. A RasGas spokesperson confirmed that "an unknown virus has affected its office systems" since Monday 27 August. RasGas confirmed the situation by fax yesterday. "RasGas is presently experiencing technical issues with its office computer systems," said the RasGas fax seen by Oil & Gas Middle East, dated 28 August. "We will inform you when our system is back up and running."

http://www.arabianbusiness.com/cyber-attack-takes-qatar-s-rasgas-offline-471345.html

http://www.bloomberg.com/news/2012-08-30/virus-shuts-rasgas-office-computers-lng-output-unaffected-1-.html

Indian gov ponders restrictions on Chinese networking gear
2012-08-30

The Indian government is set to become the latest global power to restrict the use of Chinese-built telecoms and internet infrastructure technology, in what could be another blow to the ambitions of Huawei and ZTE as they look to grow abroad. The country's telecoms minister, Kapil Sibal, is currently considering the findings of a report submitted by his department which assessed 15 countries according to various trade and strategic factors, the India Express reported. China apparently scored highly on trade value but was bumped down when it came to a strategic assessment. The report therefore recommended that imports from China be restricted to hardware such as mobile phones, laptops and USB dongles, while technology in key strategic areas such as telecoms and broadband infrastructure, security and cloud computing be obtained from other countries.

http://www.theregister.co.uk/2012/08/30/india_china_telecoms_import_row/

Attackers Pounce on Zero-Day Java Exploit
2012-08-28

Attackers have seized upon a previously unknown security hole in Oracle's ubiquitous Java software to break into vulnerable systems. So far, the attacks exploiting this weakness have been targeted and not widespread, but it appears that the exploit code is now public and is being folded into more widely-available attack tools such as Metasploit and exploit kits like BlackHole. News of the vulnerability (CVE-2012-4681) surfaced late last week in a somewhat sparse blog post by FireEye, which said the exploit seemed to work against the latest version of Java 7, which is version 1.7, Update 6. This morning, researchers Andre' M. DiMino & Mila Parkour published additional details on the targeted attacks seen so far, confirming that the zero-day affects Java 7 Update 0 through 6, but does not appear to impact Java 6 and below. Initial reports indicated that the exploit code worked against all versions of Internet Explorer, Firefox and Opera, but did not work against Google Chrome. But according to Rapid 7, there is a Metasploit module in development that successfully deploys this exploit against Chrome (on at least Windows XP).
http://krebsonsecurity.com/2012/08/attackers-pounce-on-zero-day-java-exploit/

Connecting the Dots After Cyberattack on Saudi Aramco
2012-08-27

Publicly released details of a cyberattack on Saudi Aramco, the world's largest oil producer, appear to confirm reports that critical data on three-quarters of the company's PCs was replaced with the image of a burning American flag. In a statement on Sunday, Khalid al-Falih, Aramco's chief executive, said Aramco had restored its main internal network services after they were "impacted on Aug. 15, 2012, by a malicious virus that originated from external sources and affected about 30,000 workstations." That seemed to confirm a version of events put forth by the hackers who had claimed responsibility for the attack. The hackers, who called themselves Cutting Sword of Justice, said that they had slipped a malicious virus into Saudi Aramco on Aug. 15 that destroyed 30,000 computers.

http://bits.blogs.nytimes.com/2012/08/27/connecting-the-dots-after-cyberattack-on-saudi-aramco/

Infamous hacker Sabu gets six-month sentencing delay for helping Feds
2012-08-22

Sabu, the world's most infamous hacker-turned-traitor to his cause, has been given a six-month reprieve for sentencing on 12 counts of violating the law, after his hacker group LulzSec broke into the servers and systems of companies worldwide. Sabu is the hacker nom de plume of 28-year-old New Yorker Hector Monsegur, an unemployed father of two who allegedly commanded a loosely organized, international team of perhaps thousands of hackers from his nerve center in a public housing project on New York's Lower East Side. After the FBI unmasked Monsegur in June of 2011, he became a cooperating witness and helped bring down the crew from within, FoxNews.com exclusively revealed in March. It was unclear from Tuesday's court filings whether Monsegur continues to be active online or is simply aiding the government in its prosecutions of those already arrested, according to Wired.

A court filing by U.S. district attorney Preet Bharara to judge Loretta A. Preska said only that Monsegur was cooperating.

http://www.foxnews.com/tech/2012/08/22/infamous-hacker-sabu-gets-six-month-delay-for-playing-ball/

U.S. looks into claims of security flaw in Siemens gear
2012-08-22

The U.S. government is looking into claims by a cyber security researcher that flaws in software for specialized networking equipment from Siemens could enable hackers to attack power plants and other critical systems. Justin W. Clarke, an expert in securing industrial control systems, disclosed at a conference in Los Angeles on Friday that he had figured out a way to spy on traffic moving through networking equipment manufactured by Siemens' RuggedCom division. The Department of Homeland Security said in an alert released on Tuesday that it had asked RuggedCom to confirm the vulnerability that Clarke, a 30-year-old security expert who has long worked in the electric utility field, had identified and identify steps to mitigate its impact. RuggedCom, a Canadian subsidiary of Siemens that sells networking equipment for use in harsh environments such as areas with extreme weather, said it was investigating Clarke's findings, but declined to elaborate.

http://www.reuters.com/article/2012/08/22/ctech-us-cybersecurity-siemens-idCABRE87L02F20120822

Officials: Federal Agencies Often Don't Share Tips on Potential Terrorist Activity
2012-08-17

Nearly half of federal agencies are not sharing documented incidents of potential terrorist activity with U.S. intelligence centers, according to officials in the Office of the Director of National Intelligence. The Homeland Security and Justice departments since 2008 have been teaching federal officials and police to deposit, through a secure network, reports of suspicious behavior while being mindful of civil liberties. The point of the technology is to piece together terrorist plots before they are executed. But, some criminal justice experts say, a major obstacle is dampening the effectiveness of the initiative. Work is slow-going in connecting local agencies to fusion centers, intelligence facilities partly funded by the government that vet reports for possible distribution through the Nationwide Suspicious Activity Reporting Initiative. The system is a virtualized inventory of tips that any federal, state, or local government authority can search.

http://www.nationaljournal.com/nationalsecurity/officials-federal-agencies-often-don-t-share-tips-on-potential-terrorist-activity-20120817

Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload
2012-08-09

A newly uncovered espionage tool, apparently designed by the same people behind the state-sponsored Flame malware that infiltrated machines in Iran, has been found infecting systems in other countries in the Middle East, according to researchers. The malware, which steals system information but also has a mysterious payload that could be destructive, has been found infecting at least 2,500 machines, most of them in Lebanon, according to Russia-based security firm Kaspersky Lab, which discovered the malware in June.

http://www.wired.com/threatlevel/2012/08/gauss-espionage-tool/

http://money.msn.com/business-news/article.aspx?feed=OBR&date=20120809&id=15432837

http://economictimes.indiatimes.com/tech/internet/article-show/15421781.cms

http://www.securelist.com/en/analysis/204792238/

http://www.securelist.com/en/blog/208193767/

http://usa.kaspersky.com/threats/gauss

Pentagon proposes more robust role for its cyber-specialists
2012-08-09

Currently, the military is permitted to take defensive actions or to block malicious software — such as code that can sabotage another computer — only inside or at the boundaries of its own networks. But advances in technology and mounting concern about the potential for a cyberattack to damage power stations, water-treatment plants and other critical systems have prompted senior officials to seek a more robust role for the department's Cyber Command. The proposed rules would open the door for U.S. defense officials to act outside the confines of military-related computer networks to try to combat cyberattacks on private computers, including those in foreign countries.

http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html

Kaspersky developing new secure SCADA operating system
2012-08-07

Russian antivirus firm Kaspersky Lab is on the hunt for developers to complete a secure operating system that could fend off the next Stuxnet attack on industrial control systems. The company, which

earlier this year reported the discovery of 'super-weapon' malware Flame, is seeking a developer and analyst to help create an operating system that prevents untrusted items from executing on process control systems (PCS), according to Russian recruitment site, HeadHunter. The postings say the Kaspersky Lab project "is developing rapidly". It wants recruits with experience programming PCS and Supervisory Control And Data Acquisition (SCADA) systems, implementing industrial networking and communications protocols, and knowledge of Siemens, Emerson, Omron, ABB and other programmable logic controllers.

http://www.cso.com.au/article/432846/kaspersky_developing_new_secure_scada_operating_system/#closeme

Iranian state goes offline to dodge cyber-attacks
2012-08-05

Iran is to move key ministries and state bodies off the worldwide internet next month in an effort to shield them behind a secure computer wall from disruptive cyber attacks like the Stuxnet and Flame viruses. "The establishment of the national intelligence network will create a situation where the precious intelligence of the country won't be accessible to these powers," Mr Taghipour told a conference on Sunday at Tehran's Amir Kabir University. He described the move as the first phase of a project to replace the global internet with a domestic intranet system scheduled to be completed within 18 months.

http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-goes-offline-to-dodge-cyber-attacks.html

http://www.rt.com/news/iran-internet-intranet-security-938/

New Model Sparks Safeguards to the Grid
2012-08-02

A significant modernization effort underway across the national electric grid is seeking a balance between strong cybersecurity capabilities and affordable protections across the sector. To help the private industries that generate and transmit electrical power with their efforts to develop safeguards that correspond with new technologies, the U.S. departments of Energy and Homeland Security have issued a model of voluntary measures.

http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=3032&zoneid=357

Vulnerability disclosure framework for industrial control systems
2012-08-02

The Industrial Control Systems Joint Working Group (ICSJWG) published "The Industrial Control Systems Common Vulnerability Disclosure Framework", which is a significant step towards standardization of vulnerability disclosure policies for ICS vendors and system integrators. ICSJWG was established by the Department of Homeland Security's National Cyber Security Division's Control Systems Security Program (CSSP) to assist the industrial control systems stakeholders in better information sharing, raising collaborative efforts and reducing risks related to critical infrastructure. The newly published framework is to be used as a consensus-based foundation for all involved parties in developing standardized vulnerability disclosure policies. As the framework is aimed towards a diverse set of systems, its content isn't mandatory but should be used as a valuable starting point towards responsible disclosure.

http://www.net-security.org/article.php?id=1748

UPCOMING EVENTS

October

ICSJWG 2012 Fall Meeting
October 15–18, 2012
Grand Hyatt Denver
Denver, Colorado
ICSJWG Fall 2012 Meeting Information
Registration

ICSJWG 2012 Fall Meeting—Intermediate Cybersecurity for Industrial Control Systems
October 18, 2012
Denver, Colorado
Course Description
Registration

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/

November

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (5 days)
November 5–9, 2012
Idaho Falls, ID
Course Description
Registration

December

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (5 days)
December 3–7, 2012
Idaho Falls, ID
Course Description
Registration

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 AUGUST 2012

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

- Security Researcher Justin W. Clarke of Cylance Inc, ICSA-12-243-01, GarrettCom – Use of Hard-Coded Password (August 30, 2012)
- Researchers Billy Rios and Terry McCorkle, ICSA-12-228-01, Tridium Niagara Multiple Vulnerabilities (August 14, 2012)
- Siemens self-reported, ICSA-12-227-01, Siemens COSMOS Database Privilege Escalation Vulnerability, (August 14, 2012)
- Siemens self-reported, ICSA-12-214-01, Siemens Synco OZW Default Password, (August 01, 2012)

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2012

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

Justin W. Clarke
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)
Alexandr Polyakov
Carlos Mario Penagos Hollmann
Alexey Sintsov
Adam Hahn
Manimaran Govindarasu
Jürgen Bilberger
Reid Wightman
Luigi Auriemma
Dan Tentler
Nadia Heninger
Zakir Duremeric
Eric Wustrow
J.Alex Halderman
Michael Messner
Wesley McGrew