ICS-CERT MONTHLY MONITOR

August 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

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

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/

INCIDENT RESPONSE ACTIVITY

VULNERABILITY OF INTERNET FACING MEDICAL DEVICES

Internet facing medical devices may have a very similar security risk profile to industrial control systems (ICSs). ICSs and medical devices are valuable equipment, often critical to the viability of the system to which they are attached. In each case, lives may depend on the devices functioning correctly. Both are increasingly being monitored remotely, which means enabling a connection to the Internet. This poses security risks when proper configuration and remote connectivity best practices are not followed.

A targeted exploit has the potential to impact a medical facility or specific equipment. In order to protect patients, large healthcare providers must take steps to remove wireless medical devices and critical systems from direct Internet access. Manufacturers of medical devices should also evaluate the security of implanted medical systems and their cyber vulnerabilities.

ICS-CERT was recently notified of an Internet facing medical device that was potentially vulnerable to a cyber attack. This device was located at a US university, and it is still unclear if it was actually in use or intended for research. ICS-CERT contacted the system administrator, who resolved the issue.

This example highlights the risk associated with connecting critical devices to the Internet, whether they are ICS networks or implantable medical devices.

ICS-CERT recommends all electronic devices be subjected to testing and evaluation before they are deployed; the more critical the device's operation, the more carefully the device should be scrutinized. If your company does not have the capability to perform this type of testing, ICS-CERT advises contacting one of the many private companies that specialize in providing these types of services.

ICS-CERT previously published an alert on the Web page that addresses the increased threat to ICSs, which contains information and mitigation strategies directed at securing Internet facing devices.

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.

INDIA'S GRID FAILURE: A POWERFUL REMINDER

In July, what appears to be more demand than supply caused India's electrical grid to collapse, and almost half of India's population lost power. The series of events that caused cascading failures throughout the grid began in the early morning of July 30, 2012, when circuit two of the 400 kV Bina-Gwalior power line tripped; circuit one was off-line for scheduled maintenance to upgrade capacity. One estimate of the impact from that power failure was an immediate loss of approximately 32,000 MW. At the time of the failure, the cause was unknown; however low grid frequency indicated that power consumption was greater than available capacity. In addition, the Bina-Gwalior circuit one went off-line just as farmers were using greater than normal power for irrigation due to low rainfall. When the outage occurred speculation was rampant, including rumors that states were drawing more than their grid allotment. The initial outage affected more than 300 million people, making it the largest outage in the last decade. The consequences were far reaching, affecting air terminals, railways, commuter transportation, hospitals, water and waste water systems, and other critical infrastructure. Many industries were forced to transfer to onsite power production from diesel generators.

On July 31, as the affected grid segments were being restored, another outage occurred near the Taj Mahal. Once again, low grid frequency indicated more power demand than supply. As a result of the combined failures, nearly 600 million people were without power in 20 of India's 28 states. The outages severely impacted multiple sectors, stranding rail passengers between stops, and leaving miners stuck underground. Lack of power created massive traffic jams in major cities—because of traffic light outages— that complicated rescue and power restoration efforts.

In India, the national grid is considered to be unreliable, leading many Indians to depend on alternate power sources. Vital services commonly use double, and sometimes triple the number of recommended uninterruptible power supplies (UPS) for their sector. In addition the use of diesel generators to supply their power is common. The fact that UPSs and diesel generators are so common probably dampened the effects of the power outage. Many large companies and critical infrastructure industries have segregated themselves from the vulnerable state-run electric grid. Companies have spent about $29 billion to shield their plants from electrical disruptions by building their own independent infrastructure and power stations. Total grid instability in India is suspected to cost critical manufacturing a total of 40 percent decreased productivity every year.

The overwhelming demand on India's national electrical grid was a major factor in the subsequent cascading failure of nearly the entire system. The power supply challenge was also complicated by the theft of power; industrial corporations and residential dwellings illegally siphon power, accounting for nearly 42 percent of transmission losses in Dehli alone. India was unable to meet the growing demand for electricity as the economy continued to expand and devirsify on outdated infrastructure. As the demand outgrew system capacity, grid components failed, creating a cascading failure scenario as other connected substations, relays, and power plants tripped offline. The widespread power outage affected multiple industries and critical infrastructure sectors, and most likely will happen again.

Visibility into the power grid operation is essential, providing insight into supply and demand, and allowing utilities to adjust accordingly. Industrial control systems and robust communication networks help to achieve good visibility. While a cyber attack was NOT the determined cause of the latest Indian grid failure, nefarious activities could amplify the overall grid fragility, leading to more widespread outages. Modernization and even privatization of India's national grid could help to enhance protection and minimize future blackouts.

U.S. critical infrastructure asset owners and operators are encouraged to visit the ICS-CERT Web page for the latest reported vulnerability information, alerts, and advisories concerning cyber vulnerabilities that could affect the electrical sector.

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.

CSSP NEWS

INDUSTRY DEVELOPS A DISCLOSURE POLICY

The Industrial Control Systems Joint Working Group (ICSJWG) Vendor subgroup released the initial version of the Common Industrial Control System Vulnerability Disclosure Framework, which provides a consensus based foundation for ICS vendors and integrators working to develop a vulnerability disclosure policy. The desire to demonstrate a strong commitment to security and to positive handling of vulnerabilities has led to a focus on responsible disclosure. The document is not intended to be prescriptive. Vendors have unique challenges related to how their products are used and the potential risks inherent in different disclosure paths. The Framework provides recommended ranges and formats for different aspects of the disclosure process.

UPDATES TO ICS-CERT VULNERABILITY DISCLOSURE POLICY

ICS-CERT recently updated its Vulnerability Disclosure Policy to facilitate more effective coordination of vulnerabilities that impact ICS. The goal of this policy change is to balance the control system community's need for information about security vulnerabilities with the vendor community's need for time to respond effectively.

The most siginificant update to this policy involves those situations in which a vendor is not responsive or is unable to establish a reasonable timeframe for remediation. In that case, ICS-CERT may disclose vulnerabilities 45 days after making the initial contact, regardless of vendor patch or workaround availability. The final vulnerability disclosure determination will be based on the best interests of the overall ICS community.

To report a vulnerability to ICS-CERT, please email ics-cert@hq.dhs.gov or call 1-877-776-7585. When sending sensitive information to ICS-CERT via email, you are encouraged to encrypt your messages (ICS-CERT PGP Key).

DEF CON WRAP UP

This year's DEF CON conference in Las Vegas, Nevada, (July 26–29) celebrated the 20th anniversary of the well known hacker conference. This year the conference focused on software, hardware, wireless, medical devices, and other topics of general interest to the hacker community.

Exploiting supervisory control and data acquisition (SCADA) systems and ICS devices is not a new concept. As usual, DEF CON provided a unique opportunity to observe some of the top talent in the field. Leading cyber researchers used DEF CON venues to demonstrate their work to their peers, and the presentations often provided valuable information to attendees. Presentations at this year's DEF CON demonstrated new vulnerabilities in multiple control system products, and ICS-CERT developed two alerts and an advisory in support of those discolsures, which can be found at the following links:

ICS-ALERT-12-212-02 - WellinTech KingView User Credentials Not Securely Hashed

ICS-ALERT-12-212-01 - Kessler-Ellis Products InfiLink HMI Insufficiently Protected Credentials

ICSA-12-212-01 - ICONICS GENESIS32/BizViz Security Configuration Authentication Bypass Vulnerability

For a complete list of ICS-CERT products visit the Advisories and Alerts Archive Web page.

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-12-212-01 - KEP Infilink HMI Insufficient Password Hash

ICS-ALERT-12-212-02 - WellinTech KingView User Credentials Not Securely Hashed

ICS-ALERT-12-195-01 - Tridium Niagara Directory Traversal and Weak Credential Storage Vulnerability

ADVISORIES

ICSA-12-213-01 - Sielco Sistemi Winlog Mult Vulnerabilities

ICSA-12-212-01 - ICONICS GENESIS32-BizViz Security Configurator

ICSA-12-212-02 - Siemens SIMATIC S7-400 PN CPU DoS

ICSA-12-205-01 - Siemens WinCC Insecure SQL Server Authentication

ICSA-12-205-02 - Siemens SIMATIC STEP 7 DLL Vulnerability, (July 23, 2012)

ICSA-12-201-01 - OSIsoft PI OPC DA Interface Buffer Overflow (July 19, 2012)

ICSA-12-177-02 - Wonderware Intouch 10 DLL Hijack, (July 23, 2012)

ICSA-12-185-01 - WellinTech KingView Multiple Vulnerabilities, (July 3, 2012)

RECENT PRODUCT RELEASES (Continued)

OTHER

Cyber Intrusion Mitigation Strategies (UPDATE), ICS-TIP-12-146-01A (July 19, 2012)

The ICS-CERT Monthly Monitor June‒July 2012 issue includes highlights of activities from May and June 2012.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Def Con: How to hack all the transport networks of a country
2012-07-31
"I did not do it! I just downloaded a torrent I found when I was looking for porn," stated 24-year-old Alberto García Illera at the beginning of his Def Con presentation called "How to hack all the transport networks of a country." His talk mixed humor, knowledge, social engineering and hacking as he made it look amazingly easy to pwn all the transport networks. Illera referenced "Anatomy of a subway hack," a talk from Def Con 16 which scared enough people in power that a judge barred the MIT students from giving the presentation.

The first target was a subway station in Spain that has lots of "try me" touch surface machines to search for the fastest route or for tourist information. While this machine started off being "stupid" and "harmless" as it would not allow users to download material from the Internet, Illera said that by trying to "print," a Windows dialogue box opened that showed files, allowed for drag and drop to reach the command prompt and then connect to FTP. After taking control of this machine, they could see the router which was only secured by using the default password.
http://m.blogs.computerworld.com/cybercrime-and-hacking/20766/def-con-how-hack-all-transport-networks-country

India's Power Grid Collapses Again
2012-07-31
NEW DELHI--Much of India's electricity supply network collapsed Tuesday in the country's second major outage in two days, affecting more than 680 million people—double the population of the U.S.—and causing business losses estimated to run into the hundreds of millions of dollars.

Thousands of offices and factories had to switch to generators or shut shop, more than 200 trains were brought to a standstill while hospitals had to ask nurses to manually work critical equipment such as ventilators as 21 provinces experienced a near-total blackout that raised questions about the infrastructure in Asia's third-largest economy.

Metro rail services in the national capital of New Delhi and its suburbs were halted for several hours as well, a spokesman for the Delhi Metro Rail Corp. said. At Delhi's international airport, diesel generators kicked in automatically to ensure operations were not interrupted.
http://online.wsj.com/article/SB10000872396390444405804577560413178678898.html
http://timesofindia.indiatimes.com/liveblog/15291183.cms#liveb15294985
http://www.washingtonpost.com/world/india-blackout-on-second-day-leaves-600-million-without-power/2012/07/30/gJQA7j1LMX_story.html?hpid=z1
http://www.reuters.com/article/2012/07/31/us-india-blackout-idUSBRE86U0C520120731

Measuring DHS effectiveness monitoring chemical plant safety standards
2012-07-31
The events of 9/11 triggered a national re-examination of the security of facilities that use or store hazardous chemicals in quantities which, in the event of a terrorist attack, could put large numbers of Americans at risk of serious injury or death; the GAO issued a report on how DHS ensures compliance with chemical facilities security standards

The events of 9/11 triggered a national re-examination of the security of facilities that use or store hazardous chemicals in quantities which, in the event of a terrorist attack, could put large numbers of Americans at risk of serious injury or death.

GAO notes that DHS, as required by statute, issued regulations that establish standards for the security of high-risk chemical facilities. DHS established the Chemical Facility Anti-Terrorism Standards (CFATS) program to assess the risk posed by these facilities and inspect them to ensure compliance with DHS standards.
http://www.homelandsecuritynewswire.com/dr20120731-measuring-dhs-effectiveness-monitoring-chemical-plant-safety-standards#.UBfi7oOG-jU.twitter

Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking
2012-07-26
nCircle, the leader in information risk and security performance management solutions, today announced the results of a survey of 181 attendees of the Black Hat USA 2012 security conference in Las Vegas, Nevada.
When asked "Have you ever engaged in retaliatory hacking?" 64% said "never", 23% said "once", and 13% said "frequently".

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

The information security community is divided on the practice of retaliatory hacking. Some information security professionals believe retaliatory attacks may discourage further attacks, while others believe these attacks are only likely to escalate hostilities, and increased attacks have the potential to do irreparable damage.
http://www.marketwatch.com/story/black-hat-survey-36-of-information-security-professionals-have-engaged-in-retaliatory-hacking-2012-07-26

Air Traffic Controllers Pick the Wrong Week to Quit Using Radar
2012-07-26
It's a Twilight Zone episode waiting to happen. A commercial pilot at 30,000 feet gets sudden instructions from air traffic control on the ground that another plane is headed his way.

The pilot diverts as directed but then controllers tell him a third plane is now in his path, and then a fourth and fifth. Yet when the pilot looks out his window, he sees nothing in the sky.

This is the kind of spoofing attack that could become possible, according to security researcher Andrei Costin, who spoke at the Black Hat security conference on Wednesday about serious vulnerabilities in a new air traffic control system that is currently being deployed in the U.S. and elsewhere.

The system, known as Automated Dependent Surveillance-Broadcast, or ADS-B, uses radio frequencies for communication between one plane and another and between planes and the ground. It's already widely used in Australia, where planes are required to be ADS-B compliant by 2013, and is expected to replace radar for air traffic control of commercial planes by 2020.
http://www.wired.com/threatlevel/2012/07/adsb-spoofing/

Security scanner probes 1 million IPs per hour for scary vulns
2012-07-25
Immunity Inc. has released a security tool that can scan an astounding 1 million IP addresses per hour, discovering if they're susceptible to hacks that allow attackers to hijack servers or retrieve sensitive data.

The entry-level package of Swarm, as the service is called, is a 4U server that includes 10 virtual machines. This gives it the ability to test a huge number of IP addresses against a battery of sophisticated exploits. The software inside scales linearly, meaning two of the boxes can scan roughly twice as fast, and so on, said Dave Aitel, head of Miami-based Immunity. Prices begin in the "low six figures."
http://arstechnica.com/security/2012/07/security-scanner-probes-1-million-ips-per-hour/

Researcher releases smart meter hacking tool
2012-07-20
Security consulting firm SecureState today released a new open source hacking tool that it claims will let security researchers and penetration testers verify the security of electric utility smart meters being installed in millions of homes around the country.

The tool, called Termineter, is available for public download from SecureState's website and will be demonstrated at the BSides security event in Las Vegas next week. The company had earlier sent out a stripped down version of the tool to a limited number of individuals.

Security consultancy InGuardians had planned to publicly release details of a similar tool called OptiGuard at the Shmoocon security conference a few months ago. The company however pulled the talk at the last minute in after a unnamed smart grid vendor and several utilities expressed concern that the tool would allow hackers to exploit vulnerable smart meters.
http://www.computerworld.com/s/article/9229384/
http://thehackernews.com/2012/07/open-source-smart-meter-hacking.html

Hackers Attack Servers of Oil Companies Working in Arctic
2012-07-16
Hacker group Anonymous said it had successfully hacked into the servers of five oil and gas companies operating in the Arctic, including Gazprom and Rosneft, posting hundreds of company email addresses and passwords online.

The companies affected by the hack included Shell, BP Global, ExxonMobil, Gazprom and Rosneft, according to the statement. The hackers released the information of 190 accounts from Gazprom and 80 from Rosneft, and database access details were also made available. The hackers said the information wasn't accessed through a software vulnerability but rather through a mistake by the webmaster.

http://www.themoscowtimes.com/business/article/hackers-attack-servers-of-oil-companies-working-in-arctic/462156.html
http://www.rferl.org/content/russia-anonymous-cyberattack-energy-firms/24646750.html
http://www.gizmodo.co.uk/2012/07/oil-barons-get-a-dose-of-the-anonymous-treatment-for-melting-our-ice-caps/
http://www.webpronews.com/anonymous-targets-oil-companies-in-opsavethearctic-2012-07
http://www.wired.com/threatlevel/2012/07/oil-companies-hacked/
http://betanews.com/2012/07/16/anonymous-supports-green-peace-hacks-oil-companies/

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

Defects leave critical military, industrial infrastructure open to hacks
2012-07-13
Security researchers have blown the whistle on serious vulnerabilities in an Internet-connected system used by the US military, hospitals, and private industry to control boilers, air-conditioners, security alarms, and other critical industrial equipment.

The defects in the Niagara Framework, which links more than 11 million devices in 52 countries, could allow malicious hackers to seize control of critical infrastructure, an article published by The Washington Post warned. The vulnerabilities were unearthed by Billy Rios and Terry McCorkle, two researchers who have spent the past 18 months exposing security holes in a variety of ICS, or industrial control systems.
http://digg.com/newsbar/topnews/defects_leave_critical_military_industrial_infrastructure_open_to_hacks

Tridium's Niagara Framework: Marvel of connectivity illustrates new cyber risks
2012-07-12
Tridium's driving technology, 4 million lines of software code called the Niagara Framework, is a marvel of innovation. With the click of a mouse, Niagara enables plant managers to view video streams, high-rise superintendents to operate air conditioners and elevators, security officials to track personnel inside U.S. military facilities, and nurses to monitor medical devices in hospitals.

Last week, after more than a month of conversations with The Post, the company in a confidential security bulletin warned customers about the vulnerabilities and described ways to mitigate them.
http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html
http://www.forbes.com/sites/markgibbs/2012/07/11/if-you-use-tridiums-niagara-you-could-get-hacked

Chemical giant foils infected USB stick espionage bid
2012-07-11
An attempt to infiltrate the corporate systems of Dutch chemical giant DSM by leaving malware-riddled USB sticks in the corporation's car park has failed. Instead of plugging the discarded drives into a workstation, which would have infected the machine, the worker who first found one of the devices handed it in to DSM's IT department.
http://www.theregister.co.uk/2012/07/11/infected_usb_spyware/

Power Outage Highlights Infrastructure Vulnerability
2012-07-02
As close to 3 million inhabitants of the Washington, D.C., area hunker down for an un-air-conditioned day of triple digital temperatures after a fast-moving line of storms took out power on both sides of the Potomac, we can ponder for a moment the digital consequences of this difficult situation.
http://www.forbes.com/sites/rogerkay/2012/07/02/power-outage-highlights-infrastructure-vulnerability/

Mark Weatherford's major league cyber team
2012-07-02
Today as the first civilian cyber- security chief, Weatherford is facilitating information-sharing at the highest levels of government—alongside the White House cyber czar Michael Daniel, FBI Director Robert Mueller and Gen. Keith Alexander, director of the National Security Agency. "Gen. Alexander and Mark Weatherford see themselves as peers," says Dakin, noting the military, law enforcement agencies and DHS haven't always been on the same page.
http://www.nextgov.com/cybersecurity/2012/07/security-trust/56575/

U.S. Critical Infrastructure Cyberattack Reports Jump Dramatically
2012-06-29
U.S. critical infrastructure companies saw a dramatic increase in the number of reported cyber-security incidents between 2009 and 2011, according to a new report from the U.S. Industrial Control System Cyber Emergency Response Team (ICS-CERT).

In 2009, ICS-CERT fielded 9 incident reports. In 2010, that number increased to 41. In 2011, it was 198. Of those 198, seven resulted in the deployment of onsite incident response teams from ICS-CERT, and 21 of the other incidents involved remote analysis efforts by the Advanced Analytics Lab. Incidents specific to the water sector, when added to those that impacted multiple sectors, accounted for more than half of the incidents due to a larger number of Internet-facing control system devices reported by independent researchers, according to the report.

http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/240003029/
http://www.csmonitor.com/USA/2012/0629/Report-Cyberattacks-on-critical-US-targets-surge
http://www.govinfosecurity.com/infrastructure-incidents-on-rise-a-4918/op-1
http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/

UPCOMING EVENTS

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

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

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:

- Researchers Carlos Mario Penagos Hollmann of IOActive, Michael Messner, and Luigi Auriemma have separately identified multiple vulnerabilities, ICSA-12-213-01—Sielco Sistemi Winlog Multiple Vulnerabilities, (July 31, 2012)
- Dr. Wesley McGrew of Mississippi State University, ICSA-12-212-01—ICONICS GENESIS32-BizViz Security Configurator, (July 30, 2012)
- Siemens Self-Reported, ICSA-12-212-02—Siemens SIMATIC S7-400 PN CPU DoS, (July 20, 2012)
- Siemens Self-Reported, ICSA-12-205-01—Siemens WinCC Insecure SQL Server Authentication, (July 23, 2012)
- Siemens Self-Reported, ICSA-12-205-02—Siemens SIMATIC STEP 7 DLL Vulnerability, (July 23, 2012)
- ICSA-12-201-01—OSIsoft PI OPC DA Interface Buffer Overflow (July 19, 2012)
- Researcher Carlos Mario Penagos Hollmann of IOActive, ICSA-12-177-02—Wonderware Intouch 10 DLL Hijack, (July 23, 2012)
- Researchers Carlos Mario Penagos Hollmann of IOActive and Dillon Beresford identified multiple vulnerabilities, ICSA-12-185-01—WellinTech KingView Multiple Vulnerabilities, (July 3, 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)
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
Justin W. Clarke
Dan Tentler
Nadia Heninger
Zakir Duremeric
Eric Wustrow
J.Alex Halderman
Michael Messner
Dr. Wesley McGrew