ICS-CERT MONITOR

April/May/June 2013

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

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

I Want To

- Report an ICS incident to ICS-CERT
- Report an ICS software vulnerability
- Get information about reporting

Downloading PGP/GPG Keys
http://ics-cert us-cert gov/sites/default/files/ICS-CERT_Public_Key asc

Joining the Secure Portal

ICS-CERT encourages U S asset owners and operators to join the Control Systems compartment of the US-CERT secure portal Send your name, telephone contact number, e-mail address, and company affiliation to ics-cert@hq dhs gov requesting consideration for portal access

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

INCIDENT RESPONSE ACTIVITY

BRUTE FORCE ATTACKS ON INTERNET-FACING CONTROL SYSTEMS

On February 22, 2013, ICS-CERT received a report from a gas compressor station owner about an increase in brute force attempts to access their process control network. ICS-CERT posted an alert on the US-CERT secure portal (Control Systems Center), containing 10 IP addresses, to warn other critical infrastructure asset owners, especially in the natural gas industry, to watch for similar activity. That alert elicited additional reports from critical infrastructure owners who, using the indicators in the alert, had discovered similar brute force attempts to compromise their networks. Those new reports yielded 39 new IP addresses, which ICS-CERT included in an update to the original alert (also posted on the secure portal).

The companies reporting this activity operate gas compressor stations across the Midwest and Plains states within the US, although some of the attempts reported were solely against business networks. Log analysis from the affected entities showed a date range for the attempts between January 16, 2013, and February 23, 2013. Reports from affected entities began on February 22, 2013, with no additional reports since March 8, 2013.

While none of the brute force attempts were successful, these incidents highlight the need for constant vigilance on the part of industry asset owners and operators. The ability to detect anomalous network activity and network intrusions early in an incident greatly increases the chance of a successful mitigation and resolution.

ICS-CERT encourages industry asset owners and operators to access the alerts and advisories that ICS-CERT publishes, as well as review the other proactive Recommended Practices that are available on the ICS-CERT Web site. The Control Systems Center compartment on the US-CERT portal is an excellent resource for information on current vulnerabilities in control systems as well as indicators of compromise that companies can use to check their networks for intrusions. Companies involved with U.S. critical infrastructure can contact ICS-CERT to request secure portal accounts.

Interested parties can also receive notifications of newly released Web site products by subscribing to ICS-CERT Web site RSS feeds or by following us on Twitter.

INCIDENT RESPONSE ACTIVITY - Continued

Current Activity

Most recently, ICS-CERT has assisted critical infrastructure entities in the energy and critical manufacturing sectors[a] with response to cyber intrusion attempts and compromises related to an emerging cyber threat actor. These incidents have involved common exploitation techniques and readily available tools that have been deployed successfully against many companies to compromise networks.

ICS-CERT has provided details of these events in a comprehensive alert that was disseminated through the Control Systems Center on the US-CERT Secure Portal. This alert provided information about the:

- attack methodology
- tools, tactics, and procedures (TTPs) used by attackers
- lessons learned from incident response, and
- recommended practices and mitigation strategies for intrusion detection and improvement of existing cybersecurity.

ICS-CERT periodically releases alerts, advisories, and indicator bulletins via the Control Systems Compartment of the US-CERT Secure Portal that provides critical infrastructure constituents with information intended to be useful for network defense. Asset owners and operators involved in computer network defense can request access to the US-CERT Secure Portal by emailing ics-cert@hq.dhs.gov.

ICS-CERT recommends that critical infrastructure asset owners continually evaluate their cybersecurity posture against recommended practices available from the federal government, industry groups, vendor, and standards bodies. Asset owners should employ continual risk-based assessment of cybersecurity policies to prioritize and tailor these recommended guidelines and solutions to fit specific security, business, and operational requirements.

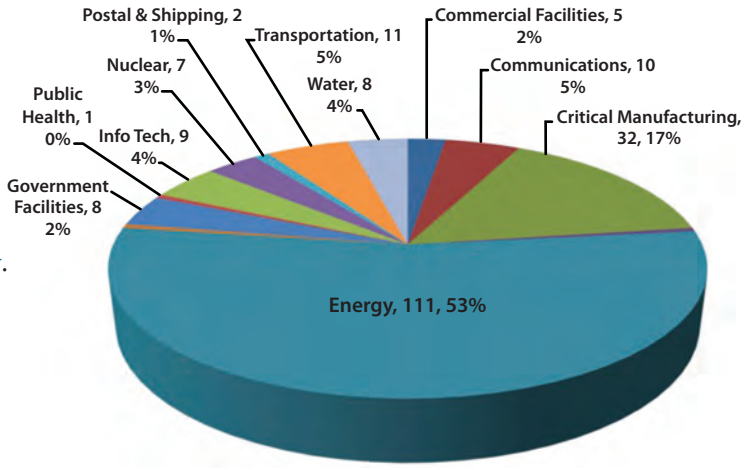
ICS-CERT recommends that organizations report cyber incidents for tracking and correlation. This enables ICS-CERT to create a big picture view of emerging malicious cyber activity, report back to the community to further situational awareness, and provide strategies for improving cyber defenses.

ICS-CERT also provides assistance to companies with the analysis of hard drives, malware, log files, and other artifacts. Indicators derived from analysis of that data are sanitized of company attribution and provided to the ICS community to support detection. Reporting incidents enables more actionable information to flow to the ICS community, and ultimately, raises awareness of cyber threats and helps to secure critical infrastructure.

Mid Year Report–Incident Response

In fiscal year 2012, ICS-CERT responded to 198 cyber incidents across all critical infrastructure sectors. Of these, 41% were in the energy sector compared to all other sectors. These incidents represented a wide variety of threats ranging from Advanced Persistent Threats (APT), to sophisticated and common malware found in the ICS environment. Other incidents in the water and commercial sectors involved Internet-facing systems with weak or default credentials.

In the first half of fiscal year 2013, (October 1, 2012–May 2013), ICS-CERT has responded to over 200 incidents across all critical infrastructure sectors. The highest percentage of incidents reported to ICS-CERT occurred in the energy sector at 53%. The critical manufacturing sector follows with 17% of reported incidents. The majority of these incidents involved attacker techniques such as watering hole attacks, SQL injection, and spear-phishing attacks. In all cases, ICS-CERT evaluates the information available to determine if successful compromise has occurred, the depth and breadth of the compromise, and the potential consequences to critical infrastructure networks.



Onsite Deployments

The majority of ICS-CERT's incident response activities are conducted remotely through the analysis of malware, log files, hard drives, emails and other artifacts provided by the affected asset owner. However, when requested, ICS-CERT deploys onsite teams to affected entities to review network topologies, identify infected systems, image drives for analysis, and collect other data as needed for follow-on analysis.

In the first half of fiscal year 2013, ICS-CERT has deployed five (5) onsite teams compared to six (6) in all of fiscal year 2012. Three of the onsites were in the energy sector and two were in the critical manufacturing sector. All of the onsite incident response engagements involved sophisticated threat actors who had successfully compromised and gained access to business networks.

While onsite, ICS-CERT analysts examined networks and artifacts to determine if ICS networks were also compromised. Unfortunately, in many cases that analysis was inconclusive because of limited or non-existent logging and forensics data from the ICS network. Whether remotely or onsite, ICS-CERT always works with the affected entities to create custom mitigations that resolve specific intrusions, and provides recommendations for hardening networks to prevent re-infection.

a While ICS-CERT is aware of specific incidents targeting the energy and critical manufacturing sectors, this activity is not limited to those sectors and could be targeted to other sectors

CONTRIBUTED CONTENT

In this edition of the Monitor, ICS-CERT is pleased to include guest submissions from Kyle Wilhoit of Trend Micro and Reid Wrightman of IOActive. Researchers interested in contributing content to ICS-CERT for consideration in future Monitor's can email ics-cert@hq.dhs.gov.

Content and opinions are those of the authors and do not represent DHS opinions, endorsements, or recommendations. The advice and instructions provided in the contributed content should be confirmed and tested prior to implementation.

YOUR SCADA DEVICES ARE BEING ATTACKED: Kyle Wilhoit, Threat Researcher, Trend Micro

There is much talk in the security community about SCADA, ICS, and whether these devices are actually attacked. Recently, Trend Micro set out to find if these devices are in fact attacked and if so, with what level of repetition. I recently gave our findings at BlackHat Europe. What's scary about the findings isn't that these devices were attacked, but the way in which these devices were attacked. Anything that is Internet facing will likely get attacked at some point.

Here is the outline of the architecture that was created to gauge attacks. In total, two honeypot architectures were built that would cover a variety of attack vectors. One architecture style was considered "high-interaction" with SCADA equipment and corresponding HMIs. In addition, the high-interaction honeypot controlled fake "gauges" that allowed attackers to think they were attacking a true rural water plant.

The second architecture was a "low-interaction" honeypot that was completely contained in the cloud. This setup accounted for traffic emulation of Modbus and DNP3 protocols as well as a custom HMI for correspondence to fake PLCs. This architecture has been subsequently expanded to account for additional variables and scenarios.

A surprising number of attacks were witnessed; the most prominent were attempts to circumvent authentication mechanisms in the HMI. In addition, one of the honeypots was spear phished by an "advanced" attacker. This was accomplished with an email sent to the "administrator" of the system. The attackers demonstrated knowledge of Modbus communications protocol because most attacks on Modbus were inject commands into the communications stream that were not issued by the controlling source. Of these attacks, roughly 17 would have been considered "catastrophic" to the water pressure pumping system.

The question that begs to be asked, "Are these attacks happening in the real world, and if they are, why are they not being disclosed?" While there is little proof these attacks are happening to real world SCADA devices, do the engineers know if the attacks are occurring? For instance, if a controller were to malfunction in a rural area of the country, would the SCADA engineer even search for the cause of the malfunction or focus primarily on getting the controller back up and running?

If any good comes out of this research, it should help prove these devices are being attacked on a fairly continuous basis. To mitigate these attacks, disconnect your SCADA/PLC devices from the Internet, use firewalls to segregate networks, and implement strong security controls in your ICS environments.

For additional details about the research performed, please visit: http://blog.trendmicro.com/trendlabs-security-intelligence/whos-really-attacking-your-ics-devices/.

WHY SANITIZE EXCESSED EQUIPMENT: Reid Wightman, IOActive

My passion for cybersecurity centers on industrial controllers–PLCs, RTUs, and the other "field devices." These devices are the interface between the integrator (e.g., HMI systems, historians, and databases) and the process (e.g., sensors and actuators). Researching this equipment can be costly because PLCs and RTUs cost thousands of dollars. Fortunately, I have an ally: surplus resellers that sell used equipment.

I have been buying used equipment for a few years now. Equipment often arrives to me literally ripped from a factory floor or even a substation. Each controller typically contains a wealth of information about its origin. I can often learn a lot about a company from a piece of used equipment. Even decades-old control equipment has a lot of memory and keeps a long record about the previous owner's process. It is possible to learn the "secret recipe" with just a few hours of work at reverse engineering a controller to collect company names, control system network layout, and production history. Even engineers' names and contact information is likely to be stored in a controller's log file. For a bad guy, the data could be useful for all sorts of purposes: social engineering employees, insider trading of company stock, and possibly direct attacks to the corporate network.

I reach out to the origin of used equipment when I find these types of information. I help them wipe the equipment, and I point them to where the rest of the equipment is being sold in an attempt to recall it before the stored information ends up in the wrong hands. I am not the only one doing this kind of work. Recently, Billy Rios and Terry McCorkle revealed surplus equipment that they had purchased from a hospital. It had much of the same information about its origin.

These situations can be prevented by sanitizing the equipment before it's released for disposal. Many equipment manufacturers should be

able to provide instructions for this process. One option may be to send the controller back to the manufacturer to be sanitized and refurbished.

A way to provide another layer of protection against information disclosure is to have a robust and well-practiced Incident Response plan. Most places that I contact are great to work with and are receptive to the information. Ignoring the issue, especially where a public utility is concerned, may be considered a violation. Set up an Incident Response program now and make sure that your process control engineers know to send equipment disposal issues through the IR group.

A great deal can be accomplished to keep a control system secure. With a little planning, proper equipment disposal is one of the cheapest things that can be done to keep proprietary process information safe.

SITUATIONAL AWARENESS

VERIZON: SUMMARY OF RESULTS AND ANALYSIS

Verizon recently published its 2013 Verizon data breach report, which contains an analysis of available 2012 incident data from 19 global organizations worldwide. Three of the supporting organizations are DHS elements 1) NCCIC, 2) US-CERT, and 3) ICS-CERT.

Recognizing that a single methodology does not exist across all contributor data, incident information for this report was coded using the Vocabulary for Event Recording and Incident Sharing (VERIS) in an attempt to create a common, anonymous aggregate dataset. Three source methods were available to normalize incident information: 1) incidents were recorded by Verizon using VERIS, 2) incidents recorded by contributors using VERIS, and 3) incident data were recoded applying VERIS to non-VERIS incident data from contributors.

Verizon had previously focused exclusively on security events resulting in confirmed data disclosure rather than the broader spectrum of all security incidents for primary analysis. This provided too small a data sample from 2012. Verizon received information from more than 47,000 incidents, but only 621 of these incidents were confirmed data disclosures with enough detail to allow a sufficient DBIR-level analysis. To make use of the previously unconfirmed/incomplete data, Verizon recoded the large body of non-VERIS-supplied incident data to VERIS. The results are included and used throughout this report.

The complete Verizon dataset used for this 2013 report spans 9 years and consists of at least 1.1 billion compromised records, spanning over 2,500 data disclosures. As a gross measure of the growth of recent data breaches, data for 2012 alone consists of 47,000 reported security incidents, 621 confirmed data disclosures and at least 44 million compromised records (those they were able to quantify).

The main body of this report demonstrated an analysis of:

- who and what is the character of the threat actors associated with reported intrusions,
- the type and style of the major threat actions observed,
- compromised assets,
- compromised data,
- attack targeting and difficulty,
- breach timelines,
- discovery methods, and
- conclusions and recommendations.

Verizon worked with the Consortium for Cybersecurity Action (CCA) to map out the most common threat action varieties in terms of the CCA Critical Security Control for Effective Cyber Defense. The report states that no one-size-fits-all solution currently exists for cybersecurity controls, but it does endorse a more general and flexible defense-in-depth security. Verizon understands that security implementation strongly depends on the organization's size, budget, risk tolerance, and business needs.

Interesting results of this study are:

- The most common existing threat actions deployed to date have improved, but new cutting edge type threat methods have not materialized.
- The list of threats against any organization can and will differ dramatically from another organization.
- Seven of the top 10 threat actions belong to the malware threat category.
- Response capabilities are extremely important in identifying and containing and mitigating issues and impacts.
- Data recovery capabilities are essential to protect business functionalities and recovery from availability issues.
- Well-designed controls do not represent a one-to-one defense against individual types of attack, but are instead measures that provide value against multiple classes of attack.
- Do not focus on just preventative controls. Detection is equally as important, and correct response is even more important.
- Focus on finding specific vulnerabilities, and blocking specific exploits is a losing battle.

- The Enhanced Mitigation Experience Toolkit (EMET) functions by blocking entire classes of exploits, rather than only specific exploits, shifting security from being reactive to proactive, and raises costs for attackers.
- Targeted attacks frequently rely on social methods to compromise people, not just computers, using social tactics such as phishing, doxing, and watering hole attacks.

This report underscores that a layered and constant approach is needed for defending, detecting, and responding to cyber incidents. No single person or group can be solely responsible for the cybersecurity of an organization. Instead, organizations should create a culture to reinforce that cybersecuriy is every employee's responsibility all the way up to the boardroom.

ADVANCES IN CSET® PERFORMANCE

The Cyber Security Evaluation Tool (CSET®) development team advanced the security tool from Version 4.1 to 5.0 giving careful consideration to the control system community conducting those evaluations.

Adopting a straightforward question set with plain language allows the tool to consistently map the standards to a single set of questions. For the user, this eliminates redundancy and reduces the time required to evaluate against multiple standards. CSET® facilitates a user self-support model and provides the most current requirements to the control system community.

In previous versions of CSET®, each standard required an independent set of questions. To perform an assessment on multiple standards the user would be required to answer a unique set of questions for each standard, resulting in potentially a few thousand questions. The new CSET® consolidates the questions and distills the information into a common set of questions that apply across all the standards. Users answer the question once, and the answer is mapped to each standard to which it applies. The user can compare answers against multiple different standards without having to re-answer the questions or re-interpret the standard.

The component questions have also been updated; some questions were outdated and no longer applicable, and others were associated with components that were only loosely related to the question. Those questions have been replaced, and the process of answering the component questions has been significantly reduced. For example, if an earlier version user included in the diagram a variety of component types, a single question might be asked multiple times; once for each type. In the new version, the question is asked only once, and the answer is set as a default for all components. The users may choose to drill down into a component type, such as application servers, and assign a value for that type. The user may also drill down to an individual device to change the response for that device.

CSET® continues to support asset owners as they work to answer significant questions about their cybersecurity posture.

Upon completion of the questionnaire, the tool provides a dashboard with a variety of charts to show specific areas of strength and weakness. The user can "drill down" from the main chart to open new windows with additional graphic and detailed information. The users can then manage their cybersecurity priorities based on the identified deficiencies ranked according to importance. The tool gives the users an overall percentage of where they stand in their cybersecurity posture and a prioritized list of where to start if the asset owners are unsure.

Future releases of CSET® are being planned based on recent customer feedback. An exciting new feature in development for CSET® 5.1 is the consolidation of questions under topic headings that can be answered as a group. The intent is to speed up the assessment process and enhance clarity for the full set of questions. Plans for later releases may include aggregation and rollup of assessments within an organization and the ability to generate cybersecurity plans based on user selected standards and security levels. Future releases will also include new sector-specific standards and updates to existing standards to match the latest versions. They will also provide ways to measure improvements over time and new resources to help asset owners make those adjustments. The CSET® team is continually striving to provide increased level of support to asset owners, operators, and vendors working to secure the Nation's critical infrastructure.

To learn more, download CSET®, or inquire about an onsite assessment, visit http://ics-cert.us-cert.gov/Assessments or email cset@hq.dhs.gov.

SECTOR SPOTLIGHT – ENERGY

This edition of the Monitor introduces a new feature that will spotlight each of the nation's 16 critical infrastructure and key resource (CIKR) sectors.

The Energy Sector provides essential enabling capability to each of the other sectors. Without energy the developed world would quickly cease to function. This sector is broadly categorized into the electricity, petroleum/oil, and natural gas segments.

The U.S. Department of Energy (DOE) is the assigned Sector-Specific Agency (SSA) with specific interface with the Office of Electricity Delivery and Energy Reliability (OE). DOE helped coordinate the preparation of the 2010 Energy Sector-Specific Plan (SSP) that is an annex to the National Infrastructure Protection Plan (NIPP). The Energy Sector envisions: "a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management

programs, coordinated response capabilities, and trusted relationships between public and private partners at all levels of industry and government."

Although more than 85 percent of the country's energy infrastructure is owned by the private sector, the U.S. Federal Government is a significant owner of energy assets and critical infrastructure. Cross-sector examples include Tennessee Valley Authority, a major owner of hydroelectric dams, nuclear and fossil power generation stations, and high-voltage transmission; Bureau of Reclamation, a major dam owner; DOE, which oversees the Strategic Petroleum Reserve and the Northeast Home Heating Oil Reserve; and power administrations such as the Western Area Power Administration and the Bonneville Power Administration.

ICS-CERT NEWS

ICS-CERT RECOGNIZED AS "SECURITY TEAM OF THE YEAR"

Recently, Marty Edwards, Director of the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), was presented SC Magazine's "Security Team of the Year" award at a ceremony held in conjunction with the RSA conference in San Francisco, California.

Marty Edwards said he was "very proud of the extraordinary work of our ICS-CERT team…" The hard work and dedication is encouraged by the growing level of trust the team receives from the private sector. Edwards went on to say, "This award recognizes the ICS-CERT and the significant progress made by the Department of Homeland Security in the area of cybersecurity coordination and information sharing between the government and private sector owners of critical infrastructure and underscores the commitment of all stakeholders to work together in this critically important area."

The ICS-CERT is part of the National Cybersecurity and Communications Integration Center (NCCIC) and serves as the preeminent federal government resource for protecting against and responding to critical infrastructure and industrial control system threats. Since ICS-CERT's inception in 2003 (originally known as the Control Systems Security Program), adversarial interest in cyber exploitation of ICS has dramatically increased, reinforcing the need for ICS-CERT capabilities and the importance of protecting critical infrastructure and key resources.

ICS-CERT's mission is to reduce risk to the Nation's critical infrastructure by increasing cybersecurity awareness and strengthening control systems security through public-private partnerships. ICS-CERT offers situational awareness to government and the private sector through the dissemination of alerts and advisories that warn of cyber threats and vulnerabilities. ICS-CERT provides cybersecurity research and analysis capabilities supporting incident handling and vulnerability coordination activities as well as incident response for asset owners and operators, and partners with the control system community to coordinate risk management efforts and serves as the focal point for information exchange.

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.

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/

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-13-091-02 Clorius Controls ICS SCADA Authentication, April 01, 2013

ICS-ALERT-13-091-01 Mitsubishi MX Overflow Vulnerability, April 01, 2013

ICS-ALERT-13-016-01A Schneider Electric Multiple Vulnerabilities, March 05, 2013

ADVISORIES

ICSA-13-149-01 Siemens SCALANCE Privilege Escalation Vulnerabilities, 5/29/2013

ICSA-13-142-01 CODESYS Gateway Use After Free, 5/22/2013

ICSA-13-140-01 Mitsubishi MX Component V3 ActiveX Vulnerability, 5/20/2013

ICSA-13-136-01 TURCK BL20 and BL67 Programmable Gateway Hard-Coded User Accounts, 5/16/2013

ICSA-13-113-01 Wonderware Information Server Vulnerabilities, 5/07/2013

ICSA-12-354-01A RuggedCom ROS Hard-Coded RSA SSL Private Key Update, 4/29/2013

ICSA-13-106-01 Matrikon A&E Historian Health Monitor Directory Traversal, 4/26/2013

ICSA-13-116-01 Galil RIO-47100 Improper Input Validation, 4/26/2013

ICSA-13-100-01 Schneider Electric MiCOM S1 Studio Improper Authorization Vulnerability, 4/10/2013

ICSA-13-098-01 Canary Labs, Inc Trend Link Insecure ActiveX Control Method, 4/8/2013

ICSA-13-095-02 Rockwell Automation Factory Talk Services Multiple Vulnerabilities, 4/5/2013

ICSA-13-095-01 Cogent Real-Time Systems Multiple Vulnerabilities, 4/5/2013

ICSA-13-091-01 Wind River VxWorks SSH and Web Server Denial of Service Vulnerabilities, 4/1/2013

ICSA-13-043-02A (UPDATE) WellinTech KingView KingMess Buffer Overflow, 3/27/2013

ICSA-13-050-01A (UPDATE) 3S CODESYS Gateway-Server Multiple Vulnerabilities, 3/27/2013

ICSA-13-084-01 Siemens CP 1604 and CP 1616 Improper Access Control, 3/25/2013

ICSA-13-067-02 Invensys Wonderware WIN-XML Exporter Improper Input Validation Vulnerability, 3/21/2013

ICSA-13-077-01A Schneider Electric PLCS Multiple Vulnerabilities, 3/20/2013

ICSA-13-079-02 Siemens WinCC 7.0 SP3 Multiple Vulnerabilities, 3/20/2013

ICSA-13-079-03 Siemens WinCC TIA Portal Vulnerabilities, 3/20/2013

ICSA-13-079-01 Schweitzer Engineering Laboratories AcSELerator Improper Authorization Vulnerability, 3/20/2013

ICSA-13-077-01 Schneider Electric PLCS Multiple Vulnerabilities, 3/18/2013

ICSA-13-053-02A Honeywell Enterprise Buildings Integrator (EBI) SymmetrE and ComfortPoint Open Manager Station, 3/14/2013

ICSA-13-038-01A 360 Systems Image Server 2000 Series Remote Root Access, 3/8/2013

ICSA-13-067-01 Indusoft Advantech Studio Directory Traversal, 3/8/2013

ICSA-13-038-01 360 Systems Image Server 2000 Series Remote Root Access, 3/6/2013

ICSA-13-053-01 Emerson DeltaV Uncontrolled Resource Consumption Vulnerability, 3/6/2013

OTHER

January/February/March 2013–ICS-CERT Monitor

Follow ICS-CERT on Twitter: @icscert

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

IOActive Discovers Backdoor Vulnerabilities in TURCK Industrial Automation Devices
2013-05-23

IOActive, Inc., a leading provider of application security, compliance and smart grid security services, today announced that company security consultant Ruben Santamarta, uncovered hard-coded user accounts that could act as backdoors in two devices from German industrial automation manufacturer, TURCK. The affected devices from TURCK, which could be exploited remotely, are the BL20 and BL67 Programmable Gateways.

http://www.ioactive.com/news-events/ioactive_discovers_backdoor_vulnerabilities_in_turck_industrial_automation_devices.html

NIST Special Publication 800-82 Revision 1 Guide to Industrial Control Systems (ICS) Security
2013-05-21

This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance , reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

http://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

The Evolution of Industrial Control System Information Sharing
2013-05-16

The Industrial Control Systems Cyber Emergency Response Team, or ICS-CERT, recently issued an advisory warning of an elevated risk of cyber-based attacks against companies that are tasked with administering systems that control elements of our nation's critical infrastructure.

The advisory is a good example of improved efforts to break down information silos between government agencies as well as improve the mechanisms to share threat information with the public sector, said Chris Blask, Chair of the Industrial Control System Information Sharing and Analysis Center (ICS-ISAC).

http://www.infosecisland.com/blogview/23156-The-Evolution-of-Industrial-Control-System-Information-Sharing html

"The cutting edge of cybercrime"—Lulzsec hackers get up to 32 months in jail
2013-05-16

LONDON, UK—The four British Lulzsec hackers—Mustafa "tflow" al-Bassam, Ryan "kayla" Ackroyd, Jake "topiary" Davis, and Ryan "ViraL" Cleary—were sentenced today to between 20 and 32 months in jail for crimes committed during Lulzsec's 50 day hacking spree in 2011. Prosecutors described the men as being at the "cutting edge of contemporary and emerging criminal offending known as cybercrime" and as "latter-day pirates."

http://arstechnica.com/tech-policy/2013/05/the-cutting-edge-of-cybercrime-lulzsec-hackers-get-up-to-32-months-in-jail/

Hacker group Anonymous plans attack on oil-and-gas industry
2013-05-16

The hacker activist group Anonymous said it plans to target the oil-and-gas sector in a June 20 operation.

"It has been a long time coming," the collective said of the event, Operation Petrol, in a video it released this week on its YouTube page.

The group said it would hone in on the United States, Canada, England, Israel, China, Italy, France, Germany, Russia and the governments of Saudi Arabia, Kuwait and Qatar.

http://thehill.com/blogs/e2-wire/e2-wire/300239-hacker-group-anonymous-plans-attack-on-oil-and-gas-industry

Honeynet Project Researchers Build Publicly Available ICS Honeypot
2013-05-15

Industrial control system and SCADA honeypots have been tried before with relative success. While those systems were enticing to hackers who hammered away on them, they were also complicated, required real ICS and SCADA gear, and weren't publicly available.

Two researchers from Norway and Denmark hope to change that dynamic with Conpot, short for Control Honeypot. Their project is a simple configuration for now, with a relatively small attack surface. They're hoping to collect data from those who take what they started, deploy it on their own critical infrastructure networks and share the findings.

http://threatpost.com/honeynet-project-researchers-build-publicly-available-ics-honeypot/

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Stuxnet worm 'increased' Iran's nuclear potential
2013-05-15

The report, published in the Royal United Services Institute (RUSI) journal, claims the Stuxnet worm exposed vulnerabilities in Iranian enrichment facilities that would otherwise have gone unnoticed, and that production actually went up in the year after it was allegedly discovered.

In an analysis of data collected by the International Atomic Energy Agency (IAEA), Ivanka Barzashka, an academic at King's College, London, argues that Iran has regrouped and improved centrifuge performance and has started enriching uranium to higher concentrations than before.

http://www.telegraph.co.uk/technology/news/10058546/Stuxnet-worm-increased-Irans-nuclear-potential html

http://www huffingtonpost.co.uk/2013/05/16/report-stuxnet-virus-may- n 3284724 html

SCADA More Secure with New Algorithm
2013-05-14

A new algorithm can detect devices not conducting their usual work. The secure distributed control program can work within SCADA systems, such as robots or PLCs, with embedded software. The software, developed by researchers at North Carolina State University, detects and then isolates a compromised device.

http://www.isssource.com/scada-more-secure-with-new-algorithm/

Advanced Persistent Threats: The New Reality
2013-05-09

There's a lot we know about advanced persistent threats, but there's a lot we don't know.

This is due in large part to the complexity of the attacks and the stealth of the attackers. Our knowledge about APTs is growing, but, unfortunately, that's because the attacks themselves are growing in frequency. Criminals using APTs want data, so the more valuable an organization's data, the more likely it is to be targeted.

http://www.darkreading.com/vulnerability/advanced-persistent-threats-the-new-real/240154502

Researchers Hack Building Control System at Google's Australian HQ
2013-05-06

Google Australia uses a building management system that's built on the Tridium Niagara AX platform, a platform that has been shown to have serious security vulnerabilities. Although Tridium has released a patch for the system, Google's control system was not patched, which allowed the researchers to obtain the administrative password for it ("anyonesguess") and access control panels.

The researchers did not test the buttons or disrupt the system, which was running off of a DSL line, but reported the issue to Google.

"We didn't want to exercise any of the management functionality on the device itself. It's pretty fragile, and we don't want to take that thing down," said Billy Rios, a researcher with security firm Cylance, who worked on the project with colleague Terry McCorkle.

http://www.wired.com/threatlevel/2013/05/googles-control-system-hacked/

New jihadi magazine appeals for help against drones
2013-05-06

A new jihadi magazine set up by militants in Afghanistan and Pakistan has appealed to Muslims around the world to come up with technology to hack into or manipulate drones, describing this as one of their most important priorities.

http://news.yahoo.com/jihadi-magazine-appeals-help-against-drones-172729788 html

Me and my job: Marty Edwards, ICS-CERT
2013-05-01

My job is to coordinate efforts between the government and the private sector, assisting asset owners and operators in the protection of the industrial control systems (ICS) within our nation's critical infrastructure.

http://www.scmagazine.com/me-and-my-job-marty-edwards-ics-cert/article/288855/

The Cyber-Dam Breaks
2013-05-01

U.S. intelligence agencies traced a recent cyber intrusion into a sensitive infrastructure database to the Chinese government or military cyber warriors, according to U.S. officials.

The compromise of the U.S. Army Corps of Engineers' National Inventory of Dams (NID) is raising new concerns that China is preparing to conduct a future cyber attack against the national electrical power grid, including the growing percentage of electricity produced by hydroelectric dams.

According to officials familiar with intelligence reports, the Corps of Engineers' National Inventory of Dams was hacked by an unauthorized user believed to be from China, beginning in January

and uncovered earlier this month.

http://freebeacon.com/the-cyber-dam-breaks/

http://www foxnews.com/politics/2013/05/01/sensitive-army-database-us-dams-compromised-chinese-hackers-suspected/

Firefox maker says British surveillance company has hijacked its brand to help spy on targets
2013-05-01

The maker of one of the Internet's most popular browsers is taking on one of the world's best known purveyors of surveillance software.

The Mozilla Foundation — responsible for the Firefox browser — accuses Britain's Gamma International Ltd. of hijacking the Firefox brand to camouflage Gamma's electronic espionage products.

Researchers have found several samples of Gamma's FinFisher spy software disguised as a Firefox file, apparently in an effort to fool computer users into believing the virus is harmless.

http://www foxnews.com/tech/2013/05/01/firefox-company-has-hijacked-brand/

Boeing links industrial control data with business IT network
2013-04-28

The Boeing Company has developed a new approach for linking business IT networks with industrial-control systems, and the initiative has spurred a standards initiative that could enable a new kind of virtual private network, reports Ellen Messmer at Network World.

Boeing uses this approach in some of its airplane manufacturing sites, but one day it could be used in hospitals, utility plants, traffic systems and oil and gas facilities. The idea is to make the data from these systems secure, even over the Internet, to enhance information-sharing opportunities and save money.

The proposed standard, the IF-MAP Metadata for ICS Security, is under consideration at the Trusted Computing Group. The existing IF-MAP protocol helps create a database of security-related information from security products. Boeing has used the protocol to integrate ICS devices--which are typically used on discrete networks--into the company's IT networks, which tend to be linked to the Internet.

http://www.fiercecio.com/story/boeing-links-industrial-control-data-business-it-network/2013-04-28

Glitch unlocks Montgomery County jail doors
2013-04-27

About 500 locks on cell doors simultaneously opened inside Montgomery County's main jail early Saturday, prompting officials to declare a security emergency that included posting about 20 police cars on the perimeter of the facility near Clarksburg.

http://m.washingtonpost.com/local/malfunctioning-locks-open-inside-maryland-jail/2013/04/27/099f7b58-af3b-11e2-98ef-d1072ed3cc27_story html

http://www npr.org/blogs/alltechconsidered/2013/03/04/173423493/street-lights-security-systems-and-sewers-theyre-hackable-too

https://www.youtube.com/watch?v=k08fnv6FbuQ

Researcvher's Serial Port Scans Find More Than 100,000 Hackable Devices, Including Traffic Lights And Fuel Pumps
2013-04-23

You probably remember serial ports as the ancient nine-pin plug you once used to hook up your mouse or joystick to your computer in the pre-USB dark ages. But tracking down devices that still use serial port connections isn't so hard, it seems. In fact, according to H.D. Moore, any hacker can find–and tamper with–more than 100,000 of them over the Internet, including critical systems ranging from traffic lights to fuel pumps to building heating and cooling systems to retail point-of-sale devices.

http://www forbes.com/sites/andygreenberg/2013/04/23/researchers-serial-port-scans-find-more-than-100000-hackable-devices-including-traffic-lights-and-fuel-pumps/

https://community rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers

Watts Bar Nuclear Plant intruder, shooting under federal probe
2013-04-22

The FBI has joined the TVA and the Nuclear Regulatory Commission investigating a trespasser who exchanged gunfire with a security officer on the property of the Watts Bar Nuclear Plant early Sunday morning. It is unclear why the intruder -- who escaped -- was there, and investigators are saying little.

But the nuclear plant, like all federal facilities, remains under high security alert in the aftermath of the Boston bombings last week, and investigators combed the area -- even with helicopters and surveillance aircraft -- for well over 12 hours Sunday.

http://www.timesfreepress.com/news/2013/apr/22/watts-bar-intruder-shooting-under-federal/

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Canada foils 'al-Qaeda inspired' terror attack on train
2013-04-22

Canada's authorities say they have arrested and charged two people with conspiring to carry out an "al-Qaeda inspired" attack on a passenger train.

http://www.bbc.co.uk/news/world-us-canada-22258191

'Aurora' Cyber Attackers Were Really Running Counter-Intelligence
2013-04-22

The attack on Microsoft looked to be a reconnaissance mission hackers were conducting to determine what type of surveillance U.S. authorities were conducting on undercover operatives through records obtained from the software giant via court orders.

http://www.cio.com.au/article/459753

Exploiting SOHO (Small Office/Home Office) Routers
2013-04-18

ISE researchers have discovered critical security vulnerabilities in numerous small office/home office (SOHO) routers and wireless access points. We define a critical security vulnerability in a router as one that allows a remote attacker to take full control of the router's configuration settings, or one that allows a local attacker to bypass authentication and take control. This control allows an attacker to intercept and modify network traffic as it enters and leaves the network.

http://securityevaluators.com//content/case-studies/routers/soho_router_hacks.jsp

Control system hack at manufacturer raises red flag
2013-04-09

CSO — An unreported attack on the energy management system of a New Jersey manufacturer has been revealed by the U.S. Cyber Emergency Response Team (US-CERT).

Intruders successfully exploited a credential storage vulnerability in the manufacturer's Tridium energy management software made by Honeywell and identified all the company's Internet facing devices, the agency reported in the latest edition of its quarterly ICS-CERT Monitor.

http://www.csoonline.com/article/731495/control-system-hack-at-manufacturer-raises-red-flag

Shodan: The scariest search engine on the Internet
2013-04-08

Unlike Google (GOOG, Fortune 500), which crawls the Web looking for websites, Shodan navigates the Internet's back channels. It's a kind of "dark" Google, looking for the servers, webcams, printers, routers and all the other stuff that is connected to and makes up the Internet.

Shodan searchers have found control systems for a water park, a gas station, a hotel wine cooler and a crematorium. Cybersecurity researchers have even located command and control systems for nuclear power plants and a particle-accelerating cyclotron by using Shodan.

http://money.cnn.com/2013/04/08/technology/security/shodan/index.html

Scientists tout advanced process to find surgical robot bugs before the bot cuts off something important
2013-04-08

When it comes to having robotic surgeons slicing around inside your brain, heart or other important body organ, surgeons and patients need to know that a software or hardware glitch isn't going to ruin their day.

That's why a new technique developed by researchers at Carnegie Mellon University and the Johns Hopkins University Applied Physics Laboratory that promises to reliably detect software bugs and verify the software safety surgical robots could be a significant development.

http://www networkworld.com/community/blog/scientists-tout-advanced-process-find-surgical-robot-bugs-bot-cuts-something-important

New Malware Targeting POS Systems, ATMs Hits Major US Banks
2013-03-27

A new malware targeting point-of-sale (POS) systems and ATMs has stolen payment card information from several US banks, researchers say. The author behind the malware appears to have links to a Russian cyber-crime gang.

http://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

South Korean banks and media report computer network crash, causing speculation of North Korea cyberattack
2013-03-20

Computer networks at major South Korean banks and top TV broadcasters crashed simultaneously Wednesday, paralyzing bank machines across the country and prompting speculation of a cyberattack by North Korea.

Screens went blank at 2 p m. (0500 GMT), the state-run Korea Information Security Agency said, and more than seven hours later some systems were still down.

Police and South Korean officials couldn't immediately determine responsibility and North Korea's state media made no immediate comments on the shutdown. But some experts suspected a cyberattack orchestrated by Pyongyang. The rivals have exchanged threats amid joint U.S.-South Korean military drills and in the wake of U.N. sanctions meant to punish North Korea over its nuclear test last month.

http://www.foxnews.com/world/2013/03/20/south-korean-banks-and-media-report-computer-network-crash/

Security vulnerability exposes confidential information of firms seeking government contracts
2013-03-19

All federal vendors registered with the General Services Administration had their companies' confidential information exposed in a massive computer security screw-up, the agency said.

The GSA, the procurement arm through which government agencies buy products and services, is conducting a "full review" of its System for Award Management after the shocking security breach, federal officials told FoxNews.com. The latest issue with the IBM-administered system, which has been plagued with problems since it was implemented last year to integrate some eight different procurement systems, was reported to GSA officials on March 8. A software patch was implemented to close the exposure of both public and non-public data, including names, taxpayer identification numbers, marketing partner information numbers and bank account details.

http://business.topnewstoday.org/business/article/5093501/

Rules for hackers: Cyberwar manual applies international law to the field of online attacks
2013-03-19

The Tallinn Manual -- named for the Estonian capital where it was compiled -- was created at the behest of the NATO Cooperative Cyber Defense Center of Excellence, a NATO think tank. It takes existing rules on battlefield behavior, such as the 1868 St. Petersburg Declaration and the 1949 Geneva Convention, to the Internet, occasionally in unexpected ways.

http://www.foxnews.com/tech/2013/03/19/rules-for-hackers-cyberwar-manual/

http://www.ccdcoe.org/249 html

U.S. Steps Up Alarm Over Cyberattacks
2013-03-13

The nation's top spies warned Tuesday of the rising threat of cyberattacks to national and economic security, comparing the concern more directly than before to the dangers posed by global terrorism. U.S. intelligence officials told a Senate hearing that the nation is vulnerable to cyberespionage, cybercrime and outright destruction of computer networks, both from sophisticated, government-sponsored assault as well as criminal hacker groups and cyberterrorists. "It's hard to overemphasize its significance," Director of National Intelligence James Clapper said, addressing members of the Senate Intelligence Committee. "These capabilities put all sectors of our country at risk—from government and private networks to critical infrastructures."

http://online.wsj.com/article/SB10001424127887323826704578356182878527280.html

UPCOMING EVENTS 2013

June

Industrial Control Systems Cybersecurity (301) Training (5 days) North American Partners
CLOSED
June 17–21, 2013
Idaho Falls, Idaho

Boston Regional Training (4 days)
June 24–27, 2013
The Volpe National Transportation Systems Center
Cambridge, Massachusetts

Because of Sequestration, the Boston Regional training course has been CANCELLED. We apologize for the inconvenience. If you have questions, contact us at cssp_training@hq.dhs.gov**.**

July

Industrial Control Systems Cybersecurity (301) Training (5 days) North American Partners
CLOSED
July 15–19, 2013
Idaho Falls, Idaho

August

Industrial Control Systems Cybersecurity (301) Training (5 days) North American Partners
August 12-16, 2013
Idaho Falls, Idaho
Course Description and Registration

September

Industrial Control Systems Cybersecurity (301) Training (5 days) North American Partners
September 9-13, 2013
Idaho Falls, Idaho

October

Industrial Control Systems Cybersecurity (301) Training (5 days) International Partners
October 7-11, 2013
Idaho Falls, Idaho
Course Description and Registration

DOCUMENT FAQ

What is the publication schedule for this digest?

ICS-CERT publishes the ICS-CERT Monitor when an adequate amount of pertinent information has been collected.

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.

COORDINATED VULNERABILITY DISCLOSURE

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

RESEARCHERS Assisting ICS-CERT with products that were published March/April/May.

ICS-CERT appreciates having worked with the following researchers:

- Siemens ProductCERT, ICSA-13-149-01 Siemens SCALANCE Privilege Escalation Vulnerabilities, 5/29/2013
- Independent researcher Nicholas Miles, ICSA-13-142-01 CODESYS Gateway Use After Free, 5/22/2013
- Independent researchers Derek Betker and Dr_IDE, ICSA-13-140-01 Mitsubishi MX Component V3 ActiveX Vulnerability, 5/20/2013
- Researcher Rubén Santamarta of IOActive, ICSA-13-136-01 TURCK BL20 and BL67 Programmable Gateway Hard-Coded User Accounts, 5/16/2013
- Researchers Timur Yunusov, Alexey Osipov, and Ilya Karpov of the Positive Technologies Research Team, ICSA-13-113-01 Wonderware Information Server Vulnerabilities, 5/07/2013
- Independent researcher Justin W. Clarke of Cylance Inc.,ICSA-12-354-01A RuggedCom ROS Hard-Coded RSA SSL Private Key Update, 4/29/2013
- Independent researcher Dillon Beresford of Cimation, ICSA-13-106-01 Matrikon A&E Historian Health Monitor Directory Traversal, 4/26/2013
- Researcher Jon Christmas of Solera Networks, ICSA-13-116-01 Galil RIO-47100 Improper Input Validation, 4/26/2013
- Researcher Michael Toecker of Digital Bond, ICSA-13-100-01 Schneider Electric MiCOM S1 Studio Improper Authorization Vulnerability, 4/10/2013
- Independent researcher Carsten Eiram of Risk Based Security, ICSA-13-095-02 Rockwell Automation FactoryTalk and RSLinx Multiple Vulnerabilities, 4/5/2013
- Researcher Kuang-Chun Hung of the Security Research and Service Institute-Information and Communication Security Technology Center (ICST), ICSA-13-098-01 Canary Labs, Inc. Trend Link Insecure ActiveX Control Method, 4/8/2013
- Researcher Dillon Beresford of Cimation, ICSA-13-095-01 Cogent Real-Time Systems Multiple Vulnerabilities, 4/5/2013
- Researchers Hisashi Kojima and Mashahiro Nakada of Fujitso Laboratories via JPCERT/CC, ICSA-13-091-01 Wind River VxWorks SSH and Web Server Denial of Service Vulnerabilities, 4/1/2013
- Researchers Lucas Apa and Carlos Mario Penagos Hollman of IOActive, ICSA-13-043-02A (UPDATE) WellinTech KingView KingMess Buffer Overflow, 3/27/2013
- Independent researcher Aaron Portnoy of Exodus Intelligence, ICSA-13-050-01A (UPDATE) 3S CODESYS Gateway-Server Multiple Vulnerabilities, 3/27/2013
- Independent researchers Christopher Scheuring and Jürgen Bilberger from Daimler TSS GmbH coordinated disclosure of the vulnerability with Siemens, ICSA-13-084-01 Siemens CP 1604 and CP 1616 Improper Access Control, 3/25/2013
- Researchers Timur Yunusov, Alexey Osipov, and Ilya Karpov of the Positive Technologies Research Team, ICSA-13-067-02 Invensys Wonderware WIN-XML Exporter Improper Input Validation Vulnerability, 3/21/2013
- Independent researcher Arthur Gervais, ICSA-13-077-01A Schneider Electric PLCS Multiple Vulnerabilities, 3/20/2013

COORDINATED VULNERABILITY DISCLOSURE

- Positive Technologies and Siemens ProductCERT, ICSA-13-079-02 Siemens WinCC 7.0 SP3 Multiple Vulnerabilities, 3/20/2013
- Researchers Billy Rios and Terry McCorkle of Cylance; Gleb Gritsai, Sergey Bobrov, Roman Ilin, Artem Chaykin, Timur Yunusov, and Ilya Karpov from Positive Technologies; and Shawn Merdinger, ICSA-13-079-03 Siemens WinCC TIA Portal Vulnerabilities, 3/20/2013
- Independent researcher Michael Toecker of Digital Bond, ICSA-13-079-01 Schweitzer Engineering Laboratories AcSELerator Improper Authorization Vulnerability, 3/20/2013
- Independent researcher Arthur Gervais, ICSA-13-077-01 Schneider Electric PLCS Multiple Vulnerabilities, 3/18/2013
- Independent researcher Juan Vazquez of Rapid7, ICSA-13-053-02A Honeywell Enterprise Buildings Integrator (EBI) SymmetrE and ComfortPoint Open Manager Station, 3/14/2013
- Independent researchers Neil Smith and Ryan Green, ICSA-13-038-01A 360 Systems Image Server 2000 Series Remote Root Access , 3/8/2013
- Independent researcher Nin3, ICSA-13-067-01 Indusoft Advantech Studio Directory Traversal, 3/8/2013
- Independent researchers Neil Smith and Ryan Green, ICSA-13-038-01 360 Systems Image Server 2000 Series Remote Root Acces, 3/6/2013
- Independent researcher Joel Langill, ICSA-13-053-01 Emerson DeltaV Uncontrolled Resource Consumption Vulnerability, 3/6/2013

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2013

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

J. Alex Halderman	Christopher Sistrunk	Mashahiro Nakada
Aaron Patterson	Dale Peterson	Michael Toecker
Aaron Portnoy	Derek Betker	Nadia Heninger
Adam Crain	Dillion Beresford	Neil Smith
Alexey Osipov	Eric Wustrow	Nicholas Miles
Andrew Brooks	Gleb Gritsa	Postive Technologies Security
Anton Popov	Hisashi Kojima	Reid Wightman
Artem Chaykin	Ilya Karpov	Roman Ilin
Arthur Gervais	Joel Langill	Rubén Santamarta
Billy Rios	Jon Christmas	Ryan Green
Bob Radvanovsky	Juan Vasquez	Sergey Bobrov
Brendan Harris	Jürgen Bilberger	Sergey Gordeychick
Carlos Mario Penagos Hollmann	Justin W. Clarke	Shawn Merdinger
Carsten Eiram	Kuang-Chun Hung (ICST)	Terry McCorkle
Cesar Cerrudo	Lucas Apa	Timur Yunusov
Christopher Scheuring	Luigi Auriemma	Zakir Durumeric