ICS-CERT MONITOR

September 2014 – February 2015

NCCIC

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

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

https://ics-cert us-cert gov/sites/default/files/documents/ICS-CERT 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, email 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

INCIDENT RESPONSE/VULNERABILITY COORDINATION IN 2014

INCIDENT RESPONSE

In Fiscal Year 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received and responded to 245 incidents reported by asset owners and industry partners.

The Energy Sector led all others again in 2014 with the most reported incidents. ICS-CERT's continuing partnership with the Energy Sector provides many opportunities to share information and collaborate on incident response efforts. Also noteworthy in 2014 were the incidents reported by the Critical Manufacturing Sector, some of which were from control systems equipment manufacturers. The ICS vendor community may be a target for sophisticated threat actors for a variety of reasons, including economic espionage and reconnaissance. Of the total number of incidents reported to ICS-CERT, roughly 55 percent involved advanced persistent threats (APT) or sophisticated actors. Other actor types included hacktivists, insider threats, and criminals. In many cases, the threat actors were unknown due to a lack of attributional data.

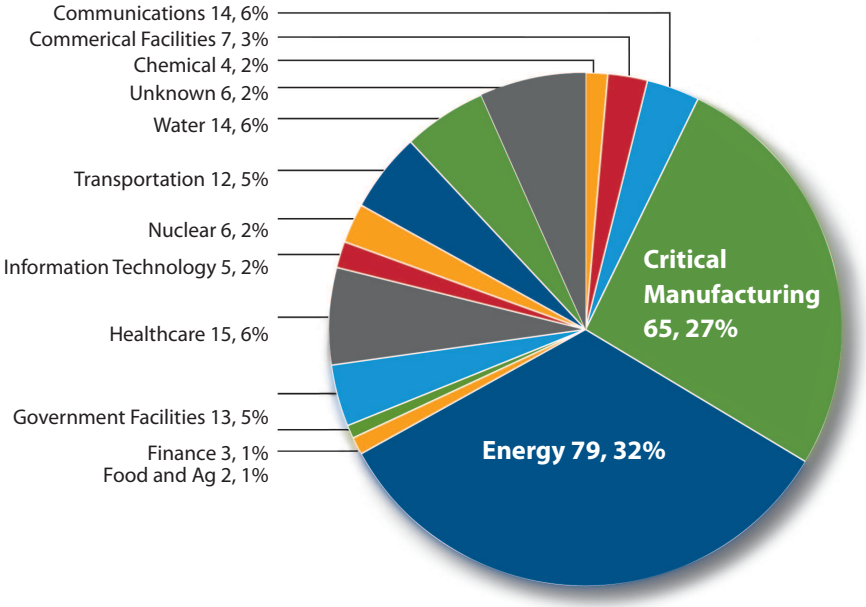


Figure 1. FY 2014 incidents reported by sector (245 total).

The scope of incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure, including but not limited to the following:

- Unauthorized access and exploitation of Internet facing ICS/Supervisory Control and Data Acquisition (SCADA) devices
- Exploitation of zero-day vulnerabilities in control system devices and software

INCIDENT RESPONSE ACTIVITY - Continued

- Malware infections within air-gapped control system networks
- SQL injection via exploitation of web application vulnerabilities
- Network scanning and probing
- Lateral movement between network zones
- Targeted spear-phishing campaigns
- Strategic web site compromises (a.k.a., watering hole attacks).

The majority of incidents were categorized as having an "unknown" access vector. In these instances, the organization was confirmed to be compromised; however, forensic evidence did not point to a method used for intrusion because of a lack of detection and monitoring capabilities within the compromised network.

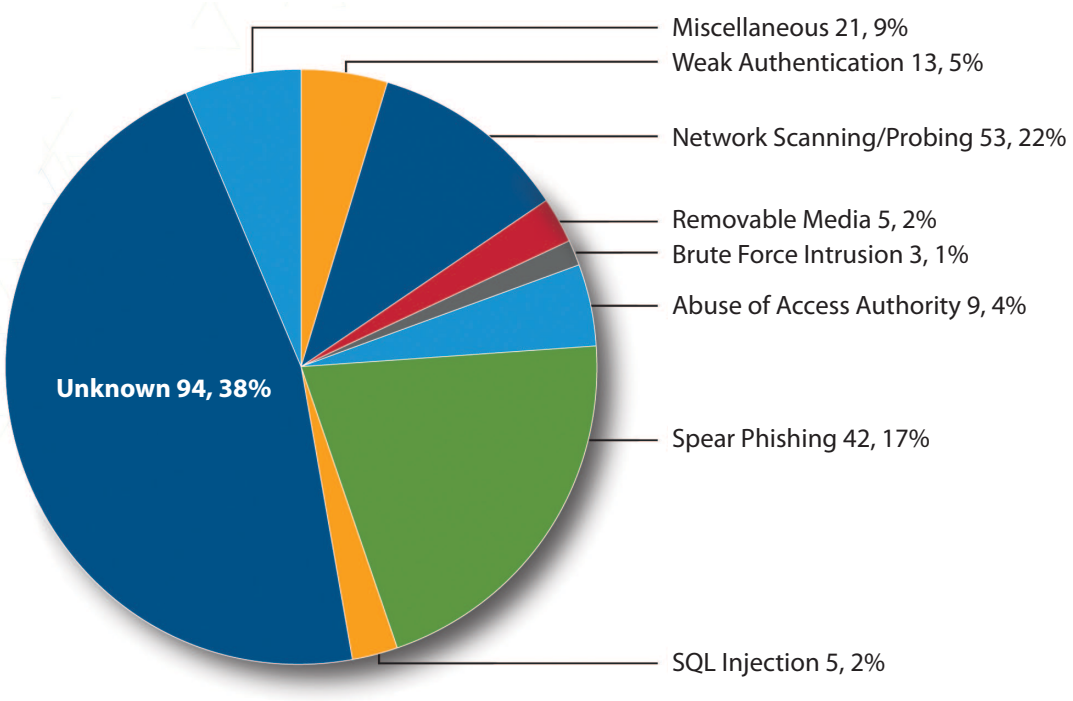


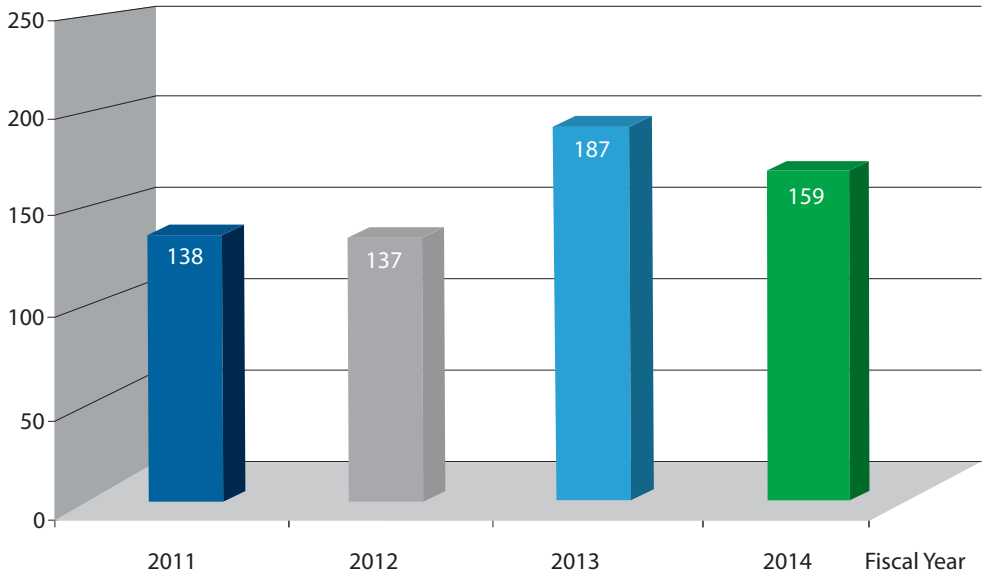
Figure 2. FY 2014 incidents reported by access vector (245 total).

The 245 incidents are only what was reported to ICS-CERT, either by the asset owner or through relationships with trusted third-party agencies and researchers. Many more incidents occur in critical infrastructure that go unreported. ICS-CERT continues to encourage asset owners to report malicious activity impacting their environment even if assistance is not needed or requested. As you report, ICS-CERT can provide situational awareness information about similar or related incidents and share data regarding the threat actor's techniques and tactics. ICS-CERT will also provide incident response services at the asset owner's request. All sensitive or proprietary information reported to ICS-CERT is protected from disclosure under the Protected Critical Infrastructure Information (PCII) program. PCII information disclosed to ICS-CERT will be handled with confidentiality while analyzing and comparing with other current threat activity. Once analysis is complete, ICS-CERT will provide the reporting entity with the latest strategies for detecting compromises and improving its defensive posture.

VULNERABILITY COORDINATION

In FY 2014, ICS-CERT received 159 reports involving vulnerabilities in control systems components and coordinated them with researchers and vendors both here in the United States and internationally. The majority of vulnerabilities that were coordinated involved systems most commonly used in the Energy Sector, followed by Critical Manufacturing and Water and Wastewater.

Authentication, buffer overflow, and denial-of-service vulnerabilities were the most common vulnerability types in FY 2014. Noteworthy among ICS-CERT's activities included the multi-vendor coordination that was conducted for the "Heartbleed" OpenSSL vulnerability. The team worked with the ICS vendor community to release multiple advisories, in addition to conducting briefings and webinars in an effort to raise awareness of the vulnerability and the mitigation strategies for preventing exploitation.



Firgure 3. Vulnerability Reports, FY 2011 - 2014.

ICS-CERT'S RESPONSE TO CYBER CAMPAIGNS AGAINST CRITICAL INFRASTRUCTURE CONTROL SYSTEMS

INCIDENT RESPONSE AND ANALYSIS

Over the last year, ICS-CERT and the Federal Bureau of Investigation (FBI) have been responding to sophisticated cyber exploitation campaigns against United States critical infrastructure ICS. These two campaigns have involved different sets of malware, both of which have used tactics to target and gain access to control systems environments. ICS-CERT is highly concerned because the sophistication of the threat actors and exploitation techniques used represent an elevated level of risk for critical infrastructure asset owners and operators.

In response, ICS-CERT has provided both onsite and remote assistance to various critical infrastructure companies to perform forensic analysis of their control systems and conduct a deep dive analysis into both Havex and Black Energy malware.

Subsequently, ICS-CERT has provided detailed information and analytic findings in various alerts that were disseminated through the Secure Portal and web site. These alerts provided information about the attack methodologies; tools, tactics, and procedures used by attackers; malware functionality; recommended practices and mitigation strategies for intrusion detection; and improvement of existing cybersecurity.

OUTREACH AND AWARENESS

In addition, to further increase awareness of the threat and provide additional context, ICS-CERT and the FBI kicked off an "Action Campaign" to conduct Secret level classified briefings for private sector critical infrastructure stakeholders across the country. ICS-CERT team members worked tirelessly to create a cohesive and unified message for stakeholders with actionable information and hand-outs at each location.

With the support and assistance of the DHS Infrastructure Protection Private Sector Clearance program, Protective Security Advisors, sector liasions and specialists, and others in DHS, ICS-CERT disseminated the invitation to stakeholders and coordinated the locations, logistics, and clearance passing for all attendees. This campaign was met with enthusiasm by the community, who responded quickly, filling every seat at all locations and requesting more briefing options.

From December 1st – 11th, teams from ICS-CERT and the FBI traveled to 15 cities across the United States, including Philadelphia, San Francisco, New York, Chicago, Denver, Los Angeles, Boston, Kansas City, Dallas, Seattle, Houston, Atlanta, Tampa, Arlington, and Washington, DC, to conduct 2-hour, Secret level briefings describing the ICS focused campaigns and the mitigation strategies for defending and detecting the activity. ICS-CERT also conducted unclassfied briefings, including unclassified webinars, to get the message out to as many stakeholders as possible.

In total, nearly 1,600 participants involved in the protection of critical infrastructure across all 16 sectors have attended the briefings.

ICS-CERT recognizes that outreach activities in the form of risk and mitigation briefings play a key role in mitigating the overall risk to critical infrastructure. ICS-CERT will continue to conduct briefings as needed to provide asset owners with the most up-to-date information on emerging threats and security measures that can be deployed to help thwart cyber-attacks and reduce risk.

TECHNICAL INFORMATION

The technical details of these two campaigns have been released in various products created by ICS-CERT. These alerts contain indicators such as IPs, Domains, Hashes, YARA rules, and detailed malware information that can be used for immediate network defense and detection.

Portal Alerts (Control Systems Center, Portal Library)

- ICS-ALERT-14-281-01CP Ongoing Sophisticated Malware Campaign Compromising ICS
- ICS-ALERT-14-281-01AP_Network_Indicators.csv
- ICS-ALERT-14-281-01CP.yara
- ICS-ALERT-14-281-01AP_DLL_Chart.csv
- ICS-ALERT-14-176-01EP -ICS Focused Malware
- Havex_Karagany_IOCs UpdateB

Web Site Alerts

- Alert (ICS-ALERT-14-281-01B) Ongoing Sophisticated Malware Campaign Compromising ICS (UPDATE B)
- Alert (ICS-ALERT-14-176-02A) - ICS Focused Malware (Update A)

ICS-CERT ASSESSMENTS

From September 2014 to February 2015, ICS-CERT conducted 37 onsite assessments to strengthen the cybersecurity posture of critical infrastructure control systems owners, operators, and control systems manufacturers in seven sectors (Table 1). Of these 37 onsite assessments, 18 were Cyber Security Evaluation Tool (CSET®) assessments, 13 were Design Architecture Review (DAR) assessments, and six were Network Architecture Verification and Validation (NAVV) assessments (Table 2).

CSET is a stand-alone software tool that enables users to assess their network and cybersecurity methodology against recognized industry and government standards, guidelines, and best practices.

The DAR assessment provides ICS asset owners with a comprehensive evaluation and discovery process, focusing on defense strategies associated with an asset owner's specific control systems network. The DAR includes an in-depth review and evaluation of the control system's network design, configuration, interdependencies, and its applications.

INCIDENT RESPONSE ACTIVITY - Continued

The NAVV assessment provides a sophisticated analysis of the asset owner's network packet-data. Using a combination of open source and commercially available tools, ICS-CERT passively analyzes the data and develops a detailed representation of the communications flows and relationships between devices.

Table 1. Assessments by sector, September 2014 through February 2015.

Assessments by Sector	2014				2015		Sept. – Feb. Totals
	September	October	November	December	January	February	
Chemical							
Commercial Facilities	2						2
Communications							
Critical Manufacturing							
Dams							
Defense Industrial Base			1		1		2
Emergency Services							
Energy	2	1	3	2		4	12
Financial Services							
Food and Agriculture							
Government Facilities					2		2
Healthcare & Public Health							
Information Technology			1				1
Nuclear Reactors, Materials & Waste							
Transportation Systems		1	1	2			4
Water and Wastewater Systems	1	6		1	3	3	14
Monthly Totals	**5**	**8**	**6**	**5**	**6**	**7**	**37 Total Assessments**

Table 2. Assessments by type, September 2014 through February 2015.

Assessments by Type	2014				2015		Sept. – Feb. Totals
	September	October	November	December	January	February	
CSET	3	5	4	2	3	1	18
DAR	1	3	1	3	2	3	13
NAVV	1		1		1	3	6
Monthly Totals	**5**	**8**	**6**	**5**	**6**	**7**	**37 Total Assessments**

PRESIDENT OBAMA SPEAKS AT NCCIC, PROPOSES NEW CYBER LEGISLATION

In an unprecedented visit to the National Cybersecurity and Communications Integration Center (NCCIC) on January 13, 2015, President Barack Obama discussed his proposal for new cybersecurity legislation "to promote the greater information sharing we need between government and the private sector." In his 10-minute speech, the President highlighted plans to build upon years of extensive discussions with industry to improve trust between the government and private sector by "making sure that government is not potentially abusing information that it's received from the private sector." He also emphasized that cyber threats pose an enormous challenge to the Nation and said, "It's one of the most serious economic and national security challenges we face as a Nation. Foreign governments, criminals, and hackers probe America's computer networks every single day." President Obama noted that protecting the Nation's critical infrastructure is essential to public health and safety, saying, "neither government, nor the private sector can defend the Nation alone. It's going to have to be a shared mission—government and industry working hand in hand, as partners."

The President outlined the three key aspects of the proposed legislation:

1) A strong, single national standard for notifying Americans when their information has been breached
2) Liability protections for companies that share information on cyber threats
3) Updating the authorities that law enforcement uses to go after cyber criminals, including assurance that "cyber criminals feel the full force of American justice, because they are doing as much damage, if not more, these days as folks who are involved in more conventional crime."

The President thanked the men and women who make up the NCCIC, which includes ICS-CERT personnel, for their dedication and 24/7 watch over the Nation's cybersecurity. "You are helping to keep the Nation safe and secure."

Read the speech at: http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent.

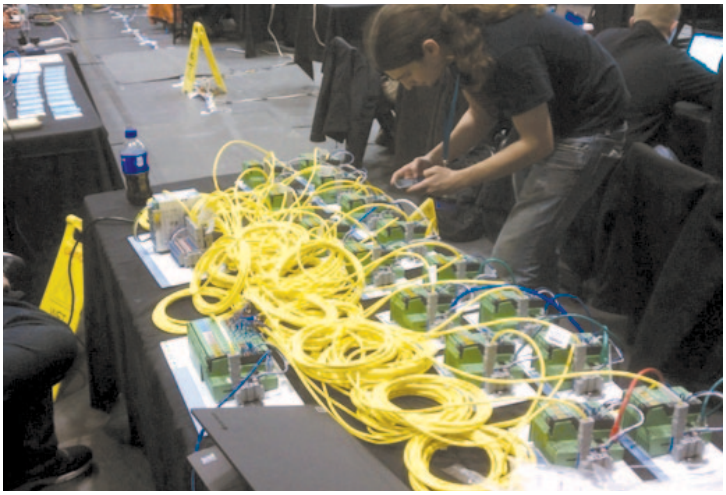
As an extension to the President's visit to the NCCIC, a White House summit was hosted by Stanford University in Palo Alto, California, on February 13, 2015. The summit brought students, government officials, and private sector leaders from the computer industry together to explore ways to improve information sharing. President Obama reemphasized the key points of the proposed legislation and the need for a partnership between government and the private sector, saying, "There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners."

The President highlighted an announcement from earlier that week concerning the creation of a new Cyber Threat Intelligence Integration Center. This new entity is analyzing and integrating and quickly sharing intelligence about cyber threats across government to improve response times. He then announced and signed a new executive order to promote information sharing about cyber threats, both within the private sector and between government and the private sector. The order is designed to encourage more companies and industries to set up organizations, or hubs, known as Information Sharing and Analysis Organizations (ISAO), where information may be shared securely. The goal is to ensure that the government can share threat information with these pre-established ISAOs more efficiently. With these functioning hubs, it will also make it easier for the government to provide companies with classified cybersecurity threat information that they need to protect their networks.

Read the speech at: http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

ICS-CERT AT NYU'S CYBER SECURITY AWARENESS WEEK CONFERENCE

This year at NYU Polytechnic School of Engineering's Cyber Security Awareness Week Conference (CSAW), ICS-CERT teamed up with Phoenix Contact to provide an ICS-based challenge for the students in attendance. Phoenix Contact provided 16 programmable logic controllers (PLCs), which the ICS-CERT team then programmed with the "Tower of Hanoi" problem. Each of the 15 teams participating was given an Ethernet cable connected to a PLC, each of which was then connected to a master PLC for status and remote reset.



To start the competition, the 15 CSAW teams were given a network connection and an IP address to a PLC. When connected to the PLC, they saw the following screen:

This web page was provided as a hint. Many of the teams reverse engineered the web page and were able to see a picture of the winning state. Despite having a view of the winning state, they did not have the token needed to submit. They had only changed temporary variables that were exported to prevent the web site from being used to modify the real values. The web interface became an unintended red herring on which many teams got stuck. The correct solution involved talking to the PLC using MODBUS, then they were able to read and write to the registers to play the game and get a secret message. This message changed depending on the state at which they were currently located. If they solved the puzzle without mistakes, they were presented with the token needed to submit.

Of the 15 teams in the competition, eight were able to solve the problem, though it was not solved by the first team until the afternoon of the final day. Several solutions discovered by various teams included the use of pymodbus and also a solution written in C.

After the competition was over, ICS-CERT's representatives had the opportunity to speak with some of the students who solved the problem. Each of them enjoyed the challenge, and many were surprised to learn that it used an actual protocol from actual control systems. After finishing the challenge, one student, with an exhausted look on his face, said, "That was a good challenge!"

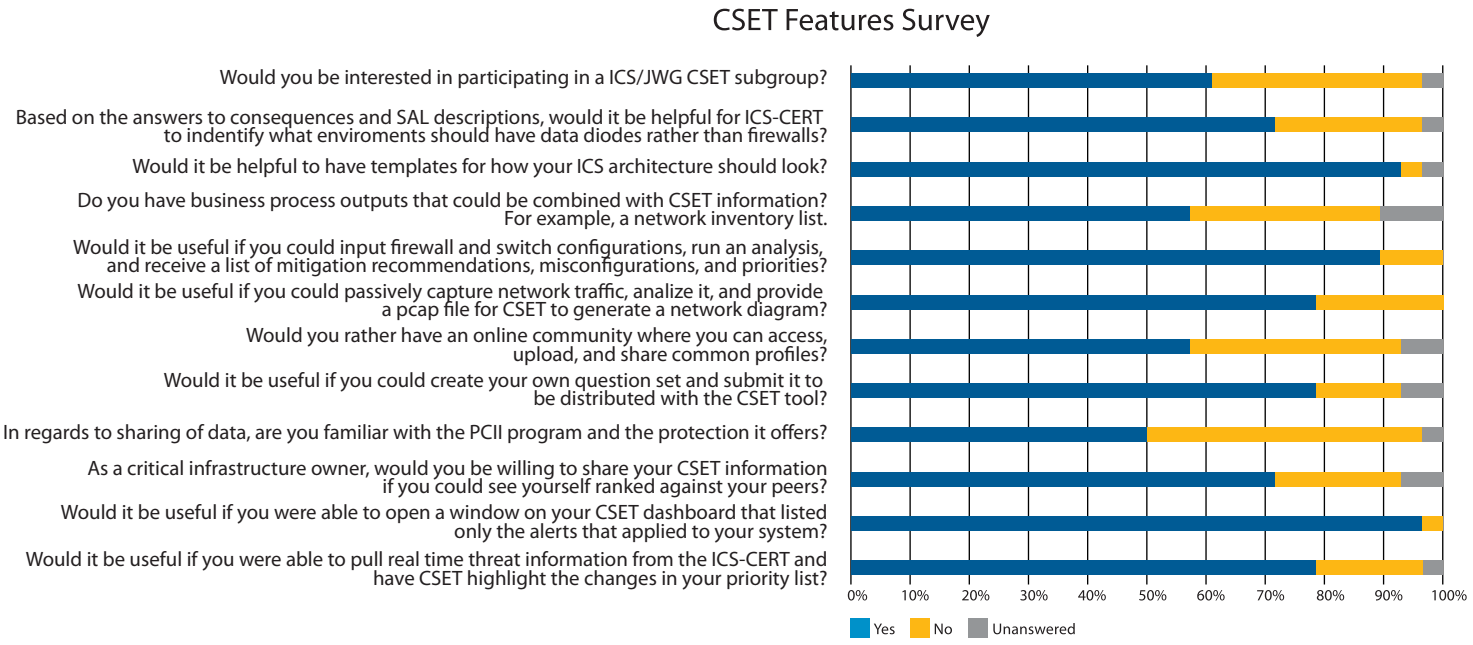
CYBERSECURITY EVALUATION TOOL

ICS-CERT continues to expand the capabilities of the Cybersecurity Evaluation Tool (CSET®), assisting asset owners to maximize their cybersecurity investment and resources. ICS-CERT released CSET 6.1 in August 2014 and CSET 6.2 in January 2015 (the next issue of the Monitor will detail CSET 6.2 updates). CSET 6.1 included the NIST Framework for Improving Critical Infrastructure Cybersecurity and NIST SP800-82 V2 (draft). In addition to supporting the baseline framework questions, this new functionality allows users to define and enter their own questions. These custom developed question sets can be redistributed via shared profile files. Industries can create their own questions and distribute them among their industry organizations. Large organizations can customize question sets for their internal use and distribute them to organizational departments or sections to aid the evaluation process based on specific needs. These custom questions can then be used to establish a baseline to trend or compare assessments.

The CSET development team gave a presentation on recent changes to CSET at the Fall 2014 Industrial Control Systems Joint Working Group (ICSJWG) meeting. The presentation included a demonstration of CSET, explained new goals for the tool, and highlighted its latest features. The presentation also described the future roadmap for CSET, elicited audience input on the new functionality, and discussed the possibility of an ICSJWG CSET subgroup. The presentation included a questionnaire concerning possible new features for CSET. The questionnaire results

(see below) indicated overwhelmingly that asset owners are looking for security guidance on control system architectures. The capability to filter ICS-CERT Alerts and Advisories to those that apply only to their individual systems was also requested.

CSET is distributed freely with the intent that users can quickly determine their cybersecurity stance and priorities and then optimize their cybersecurity improvement efforts. With these new changes, the CSET development team hopes to reduce the time asset owners spend researching what to do. Instead, it will allow them to quickly determine cybersecurity gaps and figure out how to implement security controls, mitigate discovered issues or vulnerabilities, and close any existing gaps in their cybersecurity posture. For additional information on CSET, or to download a copy, go to https://ics-cert.us-cert.gov/Assessments. The defect reporting and feature request web site is available at http://cset.inl.gov.



INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

FALL MEETING RECAP

The 2014 Fall Industrial Control Systems Joint Working Group (ICSJWG) Meeting was held October 7–9, 2014, in Idaho Falls, Idaho. The meeting served approximately 175 people from the worldwide community. This meeting included a classified briefing and tours of some of the Idaho National Laboratory facilities. Further highlights included keynote remarks by the DHS Assistant Secretary for Cybersecurity and Communications, Dr. Andy Ozment. The fall meeting also included more demonstrations and lightning round talks based on positive feedback from previous meetings. These venues allow more opportunity for participation and improved information sharing by attendants.

2015 ICSJWG MEETINGS

The planning phase for the 2015 ICSJWG meetings is underway. We are currently searching for venues and plan on hosting the first 2015 ICSJWG meeting in June. The Fall 2014 meeting was such a success that we plan on hosting the Fall 2015 meeting again in Idaho Falls. The meeting will include discussions about the security of industrial controls and critical infrastructure, including a focus on collaboration between the government and private companies and on the education of the upcoming workforce. We intend to include keynote speakers, practical demonstrations, plenary sessions, panel presentations, lightning rounds, and classified and unclassified briefings. More information about the meeting will be sent out as these special events are finalized.

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-15-041-01 Microsoft Security Bulletin MS15-011 JASBUG, 2/10/2015.
ICS-ALERT-15-030-01 Cobham Sailor 900 VSAT Buffer Overflow Vulnerability, 1/30/2015.
ICS-ALERT-14-281-01B Ongoing Sophisticated Malware Campaign Compromising ICS (Update B), 12/10/2014
ICS-ALERT-14-099-01F Situational Awareness Alert for OpenSSL Vulnerability (Update F), 12/09/2014
ICS-ALERT-14-323-01 Advantech EKI-6340 Command Injection, 11/19/2014
ICS-ALERT-14-323-02 Advantech AdamView Buffer Overflows, 11/19/2014

ADVISORIES

ICSA-15-057-01 Network Vision IntraVue Code Injection Vulnerability, 2/26/2015.
ICSA-15-055-01 Software Toolbox Top Server Resource Exhaustion Vulnerability, 2/24/2015.
ICSA-15-055-02 Kepware Resource Exhaustion Vulnerability, 2/24/2015.
ICSA-15-055-03 Schneider Electric Invensys Positioner Buffer Overflow Vulnerability, 2/24/2015.
ICSA-15-050-01 Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities, 2/19/2015.
ICSA-15-048-01 Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities, 2/17/2015.
ICSA-15-048-02 Siemens SIMATIC WinCC TIA Portal Vulnerabilities, 2/17/2015.
ICSA-15-048-03 Yokogawa HART Device DTM Vulnerability, 2/17/2015.
ICSA-14-198-03G Siemens OpenSSL Vulnerabilities (Update G), 2/17/2015.
ICSA-15-041-01 Advantech EKI-1200 Buffer Overflow, 2/10/2015.
ICSA-14-329-02D Siemens SIMATIC WinCC, PCS7, and TIA Portal Vulnerabilities (Update D), 2/10/2015.
ICSA-15-036-01 GE and MACTek HART Device DTM Vulnerability, 2/5/2015.
ICSA-15-036-02 Pepperl+Fuchs Hart Device DTM Vulnerability, 2/5/2015.
ICSA-15-012-01C CodeWrights GmbH HART Device DTM Vulnerability (Update C), 2/5/2015.
ICSA-14-353-01C Network Time Protocol Vulnerabilities (Update C), 2/5/2015.
ICSA-14-353-01-Supplement Network Time Protocol Vulnerabilities (Supplement), 2/5/2015.
ICSA-15-034-01 Siemens SCALANCE X-200IRT Switch Family User Impersonation Vulnerability, 2/3/2015.
ICSA-15-034-02 Siemens Ruggedcom WIN Vulnerability, 2/3/2015.
ICSA-15-029-01 Honeywell HART DTM Vulnerability, 1/29/2015.
ICSA-15-027-01 Magnetrol HART DTM Vulnerability, 1/27/2015.
ICSA-15-027-02 Schneider Electric Multiple Products Buffer Overflow Vulnerability, 1/27/2015.
ICSA-15-012-01B CodeWrights GmbH HART DTM Vulnerability (Update B), 1/27/2015.
ICSA-15-022-01 Siemens SIMATIC S7-1200 CPU Web Vulnerability, 1/22/2015.
ICSA-15-020-01 Siemens SCALANCE X-300/X408 Switch Family DOS Vulnerabilities, 1/20/2015.
ICSA-15-020-02 Schneider Electric ETG3000 FactoryCast HMI Gateway Vulnerabilities, 1/20/2015.
ICSA-14-345-01 Arbiter Systems 1094B GPS Clock Spoofing Vulnerability, 1/15/2015.
ICSA-14-289-02 GE Proficy HMI/SCADA CIMPLICITY CimView Memory Access Violation, 1/15/2015.
ICSA-14-287-01 GE Proficy HMI/SCADA DNP3 Driver Input Validation, 1/13/2015.
ICSA-15-013-01 Siemens SIMATIC WinCC Sm@rtClient iOS Application Authentication Vulnerabilities, 1/13/2015.
ICSA-15-013-02 Clorius Controls A/S ISC SCADA Insecure Java Client Web Authentication, 1/13/2015.
ICSA-15-013-03 Phoenix Contact Software ProConOs and MultiProg Authentication Vulnerability, 1/13/2015.
ICSA-15-013-04 GE Multilink Switch Vulnerabilities, 1/13/2015.

RECENT PRODUCT RELEASES - Continued

ICSA-15-008-01A Emerson HART DTM Vulnerability (Update A), 1/9/2015.
ICSA-15-008-02 Schneider Electric Wonderware InTouch Access Anywhere Server Buffer Overflow Vulnerability, 1/8/2015.
ICSA-14-353-01A Network Time Protocol Vulnerabilities (Update A), 12/23/2014
ICSA-14-352-01 Honeywell Experion PKS Vulnerabilities, 12/18/2014
ICSA-14-352-02 Innominate mGuard Privilege Escalation Vulnerability, 12/18/2014
ICSA-14-329-02C Siemens SIMATIC WinCC, PCS7, and TIA Portal Vulnerabilities (Update C), 12/18/2014
ICSA-13-259-01B Emerson ROC800 Multiple Vulnerabilities (Update B), 12/18/2014
ICSA-14-350-01 Schneider Electric ProClima Command Injection Vulnerabilities, 12/16/2014
ICSA-14-343-01 Yokogawa FAST/TOOLS XML External Entity, 12/09/2014
ICSA-14-343-02 Trihedral VTScada Integer Overflow Vulnerability, 12/09/2014
ICSA-14-303-02 Elipse SCADA DNP3 Denial of Service, 12/02/2014
ICSA-14-260-01A Yokogawa CENTUM and Exaopc Vulnerability (Update A), 12/02/2014
ICSA-14-329-01 MatrikonOPC for DNP Unhandled C++ Exception, 11/25/2014
ICSA-14-324-01 Advantech WebAccess Stack-based Buffer Overflow, 11/20/2014
ICSA-14-294-01 Rockwell Automation Connected Components Workbench ActiveX Component Vulnerabilities, 11/11/2014
ICSA-14-308-01 ABB RobotStudio and Test Signal Viewer DLL Hijack Vulnerability, 11/04/2014
ICSA-14-303-01 Nordex NC2 XSS Vulnerability, 10/30/2014
ICSA-14-275-01 Meinberg Radio Clocks LANTIME M-Series XSS, 10/30/2014
ICSA-14-275-02 Accuenergy Acuvim II Authentication Vulnerabilities, 10/30/2014
ICSA-14-247-01A Sensys Networks Traffic Sensor Vulnerabilities (Update A), 10/28/2014
ICSA-14-135-03A Siemens RuggedCom ROX-based Devices Certificate Verification Vulnerability, 10/16/2014
ICSA-14-198-03F Siemens OpenSSL Vulnerabilities, 10/16/2014
ICSA-14-289-01 IOServer Resource Exhaustion Vulnerability, 10/16/2014
ICSA-14-269-02 Fox DataDiode Proxy Server CSRF Vulnerability, 10/16/2014
ICSA-14-269-01A Bash Command Injection Vulnerability, 10/15/2014
Supplement-ICSA-14-269-01 Bash Command Injection Vulnerability (Supplement), 10/15/2014
ICSA-14-288-01 CareFusion Pyxis SupplyStation System Vulnerabilities, 10/15/2014
ICSA-14-259-01A Schneider Electric SCADA Expert ClearSCADA Vulnerabilities, 10/07/2014
ICSA-14-205-02A Siemens SIMATIC WinCC Vulnerabilities, 10/07/2014
ICSA-14-273-01 SchneiderWEB Server Directory Traversal Vulnerability, 09/30/2014
ICSA-14-254-02 Rockwell Micrologix 1400 DNP3 DOS Vulnerability, 09/20/2014
ICSA-14-261-01 Advantech WebAccess Vulnerabilities, 09/18/2014
ICSA-14-260-01 Yokogawa CENTUM and Exaopc Vulnerability, 09/17/2014
ICSA-14-254-01 Schneider Electric VAMPSET Buffer Overflow, 09/11/2014
ICSA-14-224-01 Ecava Integraxor SCADA Server Vulnerabilities, 09/11/2014

OTHER

ICS-CERT Monitor May – August 2014

Follow ICS-CERT on Twitter: @icscert

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

S4x15 Video: Kaspersky Control System OS
2015-02-25
http://www.digitalbond.com/blog/2015/02/23/s4x15-video-kaspersky-control-system-os/

US Coast Guard Addresses Maritime Cybersecurity Issues
2015-01-15
http://inhomelandsecurity.com/us-coast-guard-addresses-maritime-cybersecurity-issues/

End of Windows 7 Mainstream Support
2015-01-14
http://windows microsoft.com/en-us/windows/lifecycle

Enabling the Internet of Things Podcast
2015-01-13
http://csis.org/multimedia/enabling-internet-things-conversation-marty-edwards

Department of Energy Releases Energy Sector Cybersecurity Framework Implementation Guidance
2015-01-08
http://www.energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance

Measurement Data Corruption
2015-01-05
http://chemical-facility-security-news.blogspot.com/2015/01/measurement-data-corruption html
http://chemical-facility-security-news.blogspot.com/2014/12/damn-vulnerable-chemical-process html

The Biggest Security Threats We'll Face in 2015
2015-01-04
http://www.wired.com/2015/01/security-predictions-2015/
http://www.wired.com/2012/09/scada-vendor-telvent-hacked/

Leveraging The Kill Chain For Awesome
2014-12-02
http://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810
http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883
http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

Researcher Releases Database of Known-Good ICS and SCADA Files
2014-12-01
http://threatpost.com/researcher-releases-database-of-known-good-ics-and-scada-files/109652

Secure remote file access challenges
2014-11-14
http://www net-security.org/secworld.php?id=17637

Perimeter defense insufficient, security shifting, report says
2014-11-13
http://www.scmagazine.com/73-percent-of-survey-respondent-say-infosec-needs-have-changed/article/383231/
http://www nuix.com/media-release-data-breaches-inevitable-survey-findings

Hacker Lexicon: What Is a Zero Day?
2014-11-11
http://www.wired.com/2014/11/what-is-a-zero-day/
http://markmaunder.com/2014/06/16/where-zero-day-comes-from

Secure Design with Exploit Infusion
2014-11-11
http://www.sans.org/reading-room/whitepapers/application/secure-design-exploit-infusion-35587

BlackEnergy threatens U.S. infrastructure
2014-11-09
http://www.gsnmagazine.com/node/42887

Hackers Devise New Simplified Phishing Method
2014-11-05
http://www.darkreading.com/attacks-breaches/hackers-devise-new-simplified-phishing-method/d/d-id/1317242

Why Two-Factor Authentication is Too Important to Ignore
2014-10-21
http://www.infosecisland.com/blogview/24045-Why-Two-Factor-Authentication-is-Too-Important-to-Ignore.html
http://vpnhaus.ncp-e.com/2013/04/25/why-two-factor-authentication-matters/

Sandworm Team Targeted SCADA Systems: Trend Micro
2014-10-20
http://www.securityweek.com/sandworm-team-targeted-scada-systems-trend-micro
http://www.isightpartners.com/2014/10/cve-2014-4114/
http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/

Project SHINE Reveals Magnitude of Internet-connected Critical Control Systems
2014-10-07
http://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical-control-systems

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 SEPTEMBER 2014 THROUGH FEBRUARY 2015

ICS-CERT appreciates having worked with the following researchers:

- Researcher Jürgen Bilberger from Daimler TSS GmbH, ICSA-15-057-01 Network Vision IntraVue Code Injection Vulnerability, 2/26/2015.
- Adam Crain of Automatak and Chris Sistrunk of Mandiant, ICSA-15-055-01 Software Toolbox Top Server Resource Exhaustion Vulnerability, 2/24/2015.
- Adam Crain of Automatak and Chris Sistrunk of Mandiant, ICSA-15-055-02 Kepware Resource Exhaustion Vulnerability, 2/24/2015.
- Ivan Sanchez from Nullcode Team, ICSA-15-055-03 Schneider Electric Invensys Positioner Buffer Overflow Vulnerability, 2/24/2015.
- Aleksandr Timorin from Positive Technologies, ICSA-15-048-01 Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities, 2/17/2015.
- Gleb Gritsai, Roman Ilin, Aleksandr Tlyapov, and Sergey Gordeychik from Positive Technologies, ICSA-15-048-02 Siemens SIMATIC WinCC TIA Portal Vulnerabilities, 2/17/2015.
- Alexander Bolshev of Digital Security, ICSA-15-048-03 Yokogawa HART Device DTM Vulnerability, 2/17/2015.
- Enrique Nissim and Pablo Lorenzzato from the Core Security Engineering Team, ICSA-15-041-01 Advantech EKI-1200 Buffer Overflow, 2/10/2015.
- Alexander Bolshev and Svetlana Cherkasova of Digital Security, ICSA-15-036-01 GE and MACTek HART Device DTM Vulnerability, 2/5/2015.
- Alexander Bolshev of Digital Security, ICSA-15-036-02 Pepperl+Fuchs Hart Device DTM Vulnerability, 2/5/2015.
- Alexander Bolshev of Digital Security, ICSA-15-012-01C CodeWrights GmbH HART Device DTM Vulnerability (Update C), 2/5/2015.
- Google Security Team researchers Neel Mehta and Stephen Roettger coordinated multiple vulnerabilities with CERT/CC concerning the Network Time Protocol (NTP), ICSA-14-353-01C Network Time Protocol Vulnerabilities (Update C), 2/5/2015.
- IOActive coordinated with Siemens, ICSA-15-034-02 Siemens Ruggedcom WIN Vulnerability, 2/3/2015.
- Alexander Bolshev of Digital Security, ICSA-15-029-01 Honeywell HART DTM Vulnerability, 1/29/2015.
- Independent researcher Alexander Bolshev, ICSA-15-027-01 Magnetrol HART DTM Vulnerability, 1/27/2015.
- Ariele Caltabiano (kimiya) with HP's Zero Day Initiative (ZDI), ICSA-15-027-02 Schneider Electric Multiple Products Buffer Overflow Vulnerability, 1/27/2015.
- Independent researcher Alexander Bolshev, ICSA-15-012-01B CodeWrights GmbH HART DTM Vulnerability (Update B), 1/27/2015.
- Narendra Shinde of Qualys Security, ICSA-15-020-02 Schneider Electric ETG3000 FactoryCast HMI Gateway Vulnerabilities, 1/20/2015.
- Independent researcher Said Arfi, ICSA-14-289-02 GE Proficy HMI/SCADA CIMPLICITY CimView Memory Access Violation, 1/15/2015.
- Independent researcher Adam Crain of Automatak, ICSA-14-287-01 GE Proficy HMI/SCADA DNP3 Driver Input Validation, 1/13/2015.
- Independent researcher Aditya Sood, ICSA-15-013-02 Clorius Controls A/S ISC SCADA Insecure Java Client Web Authentication, 1/13/2015.
- Reid Wightman of Digital Bond, ICSA-15-013-03 Phoenix Contact Software ProConOs and MultiProg Authentication Vulnerability, 1/13/2015.
- Eireann Leverett of IOActive, ICSA-15-013-04 GE Multilink Switch Vulnerabilities, 1/13/2015.
- Independent researcher Alexander Bolshev, ICSA-15-008-01A Emerson HART DTM Vulnerability (Update A), 1/9/2015.

COORDINATED VULNERABILITY DISCLOSURE - Continued

- Google Security Team researchers Neel Mehta and Stephen Roettger, ICSA-14-353-01A Network Time Protocol Vulnerabilities (Update A), 12/23/2014.
- Alexander Tlyapov, Gleb Gritsai, Kirill Nesterov, Artem Chaykin and Ilya Karpov of the Positive Technologies Research Team and Security Lab, ICSA-14-352-01 Honeywell Experion PKS Vulnerabilities, 12/18/2014.
- Researchers Dillon Beresford, Brian Meixell, Marc Ayala, and Eric Forner, formerly of Cimation, ICSA-13-259-01B Emerson ROC800 Multiple Vulnerabilities (Update B), 12/18/2014.
- Researchers Dillon Beresford, Brian Meixell, Marc Ayala, and Eric Forner, formerly of Cimation, ICSA-13-259-01B Emerson ROC800 Multiple Vulnerabilities (Update B), 12/18/2014.
- HP's Zero Day Initiative (ZDI), ICSA-14-350-01 Schneider Electric ProClima Command Injection Vulnerabilities, 12/16/2014.
- Timur Yunusov, Alexey Osipov, and Ilya Karpov of Positive Technologies Inc., ICSA-14-343-01 Yokogawa FAST/TOOLS XML External Entity, 12/09/2014.
- An anonymous researcher working with HP's Zero Day Initiative, ICSA-14-343-02 Trihedral VTScada Integer Overflow Vulnerability, 12/09/2014.
- Independent researchers Adam Crain and Chris Sistrunk, ICSA-14-303-02 Elipse SCADA DNP3 Denial of Service, 12/02/2014.
- Tod Beardsley of Rapid7 Inc. and Jim Denaro of CipherLaw, ICSA-14-260-01A Yokogawa CENTUM and Exaopc Vulnerability (Update A), 12/02/2014.
- Adam Crain of Automatak and Chris Sistrunk of Mandiant, ICSA-14-329-01 MatrikonOPC for DNP Unhandled C++ Exception, 11/25/2014.
- Ricardo Narvaja from Core Security Consulting Services, ICSA-14-324-01 Advantech WebAccess Stack-based Buffer Overflow, 11/20/2014.
- Independent researcher Andrea Micalizzi working through ZDI, ICSA-14-294-01 Rockwell Automation Connected Components Workbench ActiveX Component Vulnerabilities, 11/11/2014.
- Ivan Sanchez of WiseSecurity Team, ICSA-14-308-01 ABB RobotStudio and Test Signal Viewer DLL Hijack Vulnerability, 11/04/2014.
- Independent researcher Darius Freamon, ICSA-14-303-01 Nordex NC2 XSS Vulnerability, 10/31/2014.
- Martem Telecontrol Systems security researcher Aivar Liimets, ICSA-14-275-01 Meinberg Radio Clocks LANTIME M-Series XSS, 10/30/2014.
- Independent researcher Laisvis Lingvevicius, ICSA-14-275-02 Accuenergy Acuvim II Authentication Vulnerabilities, 10/30/2014.
- Researcher Cesar Cerrudo of IOActive, ICSA-14-247-01A Sensys Networks Traffic Sensor Vulnerabilities (Update A), 10/28/2014.
- Chris Sistrunk of Mandiant and Adam Crain of Automatak, ICSA-14-289-01 IOServer Resource Exhaustion Vulnerability, 10/16/2014.
- Tudor Enache of HelpAG, ICSA-14-269-02 Fox DataDiode Proxy Server CSRF Vulnerability, 10/16/2014.
- Independent researcher Billy Rios, ICSA-14-288-01 CareFusion Pyxis SupplyStation System Vulnerabilities, 10/15/2014.
- Independent researcher Aditya Sood, ICSA-14-259-01A Schneider Electric SCADA Expert ClearSCADA Vulnerabilities (Update A), 10/07/2014.
- Researchers Sergey Gordeychik, Alexander Tlyapov, Dmitry Nagibin, and Gleb Gritsai of Positive Technologies, ICSA-14-205-02A Siemens SIMATIC WinCC Vulnerabilities (Update A), 10/07/2014.
- Independent researcher Billy Rios, ICSA-14-273-01 Schneider WEB Server Directory Traversal Vulnerability, 9/30/2014.
- Independent researcher Matthew Luallen of CYBATI, ICSA-14-254-02 Rockwell Micrologix 1400 DNP3 DOS Vulnerability, 9/30/2014.
- Researcher Ricardo Narvaja of Core Security Technologies, ICSA-14-261-01 Advantech WebAccess Vulnerabilities, 9/18/2014.
- Aivar Liimets of Martem AS, ICSA-14-254-01 Schneider Electric VAMPSET Buffer Overflow, 9/11/2014.
- Independent researcher Andrea Micalizzi, ICSA-14-224-01 Ecava Integraxor SCADA Server Vulnerabilities, 9/11/2014.
- Independent researcher Aditya Sood, ICSA-14-259-01A Schneider Electric SCADA Expert ClearSCADA Vulnerabilities (Update A), 10/07/2014.

COORDINATED VULNERABILITY DISCLOSURE - Continued

- Researchers Sergey Gordeychik, Alexander Tlyapov, Dmitry Nagibin, and Gleb Gritsai of Positive Technologies, ICSA-14-205-02A Siemens SIMATIC WinCC Vulnerabilities (Update A), 10/07/2014.
- Independent researcher Billy Rios, ICSA-14-273-01 Schneider WEB Server Directory Traversal Vulnerability, 9/30/2014.
- Independent researcher Matthew Luallen of CYBATI, ICSA-14-254-02 Rockwell Micrologix 1400 DNP3 DOS Vulnerability, 9/30/2014.
- Researcher Ricardo Narvaja of Core Security Technologies, ICSA-14-261-01 Advantech WebAccess Vulnerabilities, 9/18/2014.
- Aivar Liimets of Martem AS, ICSA-14-254-01 Schneider Electric VAMPSET Buffer Overflow, 9/11/2014.
- Independent researcher Andrea Micalizzi, ICSA-14-224-01 Ecava Integraxor SCADA Server Vulnerabilities, 9/11/2014.

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT

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

Adam Crain	Chris Sistrunk	Marc Ayala
Aditya Sood	Darius Freamon	Matthew Luallen
Alexander Tlyapov	Dillon Beresford	Neel Mehta
Alexey Osipov	Eric Forner	Ralf Spenneberg
Andrea Micalizzi	Glib Gritsai	Reid Wightman
Artem Chaykin	Ilya Karpov	Ricardo Narvaja
Avair Liimets	Ivan Sanchez	Sergey Gordeychick
Billy Rios	Jim Denaro	Stephen Roettger
Bob Radvanovsky	Joel Langill	Terry McCorkle
Brian Meixell	Kirill Nesterov	Timur Yunusov
Cesar Cerrudo	Laisvis Lingvevicius	Tudor Enache

DOCUMENT FAQ

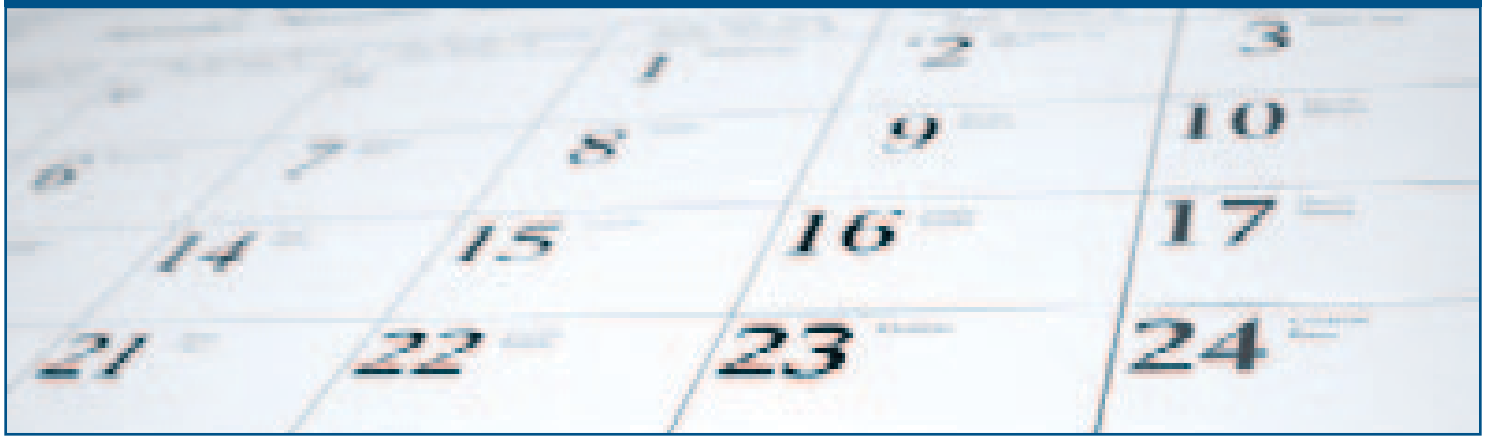
What is the publication schedule for this digest?

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.

UPCOMING EVENTS



April

Regional Cybersecurity Training for Industrial Control Systems (3 days)

April 6–9, 2015
Phoenix, Arizona USA

Course Description and Registration

April

Industrial Control Systems Cybersecurity (301) Training (5 days)

April 13–17, 2015
Idaho Falls, Idaho USA

CLOSED

May

Industrial Control Systems Cybersecurity (301) Training (5 days)

May 4–8, 2015
Idaho Falls, Idaho USA

CLOSED

For a schedule of events that the ICS-CERT is supporting and may be of interest to control system individuals involved in security, click here.

We Want To Hear From You

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