ICS-CERT MONITOR

May – August 2014

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
http://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

NOTABLE INCIDENTS

Water Treatment Facility: Control System Anomalies

ICS-CERT responded to an incident involving operational anomalies at water and wastewater treatment facilities. The asset owner reported that a control system maintenance employee had improperly accessed the control system on at least four separate occasions. According to the report, one of these instances resulted in the overflow of the systems wastewater treatment process. The asset owner requested that ICS-CERT deploy an onsite incident response team to determine if unauthorized system access had occurred and if it caused the basin to overflow.

The incident response team, in conjunction with law enforcement, performed extensive analysis of the control system and historical trending data around the four dates provided by the asset owner. The team was unable to conclusively determine if the suspected employee had unauthorized access on the date of the overflow or if that access resulted in the basin overflowing. The factors that significantly contributed to the inconclusive findings included:

- Each host did not record logon events
- Typically, only one username was used throughout the network
- A lack of network monitoring systems in place to verify the alleged activity
- Logging was not enabled or was irrelevant for any of the remote access tools seen on the hosts (pcAnywhere, RealVNC, NetVanta VPN client, Windows Remote Desktop)
- Operating system records were eliminated due to the age of reported access event.

Lessons Learned: This incident highlights the importance of detailed logging capabilities and policies related to logging analysis. Also, network administrators should implement least privilege practices and ensure that each user has unique logon credentials that provide access to only those systems the employee needs to control.

While onsite, the incident response team conducted a design and architecture review and cybersecurity assessment to thoroughly evaluate the facilities. The team identified vulnerabilities and provided recommendations to mitigate and improve the control system's security.

Sophisticated Threat Actors Compromise Manufacturer

A large critical manufacturing organization was compromised by multiple sophisticated threat actors over a period of several months. ICS-CERT received and analyzed digital media data provided by the organization and deployed an onsite incident response team to assist the organization with recovery efforts. The team performed network sweeps using indicators of compromise and identified numerous compromised hosts as well as lateral movement of the threat actors throughout their network. The response team also uncovered evidence of compromised domain accounts, which provided the intruders with privileged access throughout the network. In addition to the incident response activities, ICS-CERT analyzed its overall network architecture and provided strategies for improving the its overall defensive posture.

Lessons Learned: This organization is a conglomeration of multiple companies acquired in recent years. The acquisition and subsequent merging of multiple networks introduced latent weaknesses in network management and visibility, which allowed lateral movement from intruders to go largely undetected. The organization has over 100 entry/exit point connections to the Internet, complicating the implementation of network boundary protections. In this situation, re-architecting the network is the best approach to ensure that the company has a consistent security posture across its wide enterprise.

ICS-Focused Malware: Havex

Overview

In late June, ICS-CERT became aware of a critical infrastructure focused malware campaign by sophisticated threat actors dating back to 2011, and possibly earlier. The campaign involved multiple intrusion vectors including phishing emails and redirects to compromised web sites and software update installers on at least four industrial software vendor web sites. This attack methodology is commonly referred to as a watering hole attack. ICS-CERT's primary concerns were malware payloads focused on reconnaissance of ICS specific components. No additional ICS-specific functionality has been observed.

Various reports have indicated that organizations in the energy, manufacturing, pharmaceutical and information technology sectors are among those targeted by this campaign. However, drawing conclusions about the specific intent of targeting is not well understood as all victims have not been identified. While the specific target and motive of the campaign is unclear, the situation elevates the presence of a new and potentially evolving threat against industries operating critical infrastructure.

ICS-CERT has published detailed information about the four vendors, timelines of infections and an appendix of indicators to the US-CERT Secure Portal for critical infrastructure owners and operators. Information has also been published to the web site at: https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01.

Method of Exfiltration: OPC Module

According to reports from researchers at F-Secure and Symantec, the software installers of four critical infrastructure vendors were infected with malware known as the Havex trojan or Backdoor. Oldrea. This technique may allow an attacker access to the networks of systems that have installed the trojanized software.

Havex is a Remote Access Trojan (RAT) that communicates with a large network of compromised web sites used as Command and Control (C&C). The C&C servers deploy payloads that provide additional functionality for the intruder. ICS-CERT identified and analyzed one payload that accounts for all connected network resources, such as computers or shared resources, and uses the classic DCOM-based (Distributed Component Object Meorsdieoln) of the Open Platform Communications (OPC) standard to gather additional information about connected control system resources within each of the networks. The known components of the identified Havex payload do not appear to target devices using the newer OPC Unified Architecture (UA) standard.

In particular, the payload gathers server information that includes Class Identification (CLSID), server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth. In addition to more generic OPC server information, the Havex payload also has the capability of identifying OPC tags. OPC tags are identified when the server is queried for tag name, type, access, and ID. ICS-CERT has not found any additional functionality to control or make changes to the connected hardware; however, the payload continues to be analyzed.

ICS-CERT testing has determined that the Havex payload has caused multiple common OPC platforms to intermittently crash. This could result in a denial-of-service effect if applications rely on OPC communications. ICS-CERT recommends the following OPC risk mitigation strategies:

- Enforce strict access control lists and authentication protocols for network level access to OPC clients and servers
- Consider using OPC tunneling technologies to avoid exposure of any legacy DCOM-based OPC services
- When using OPC .NET-based communications, ensure that the HTTP server enforces proper authentication and encryption of the OPC communications for both clients and servers
- Leverage the OPC Security specification when possible.

OPC provides an open standard specification that is widely used in process control, manufacturing automation and other applications. The technology facilitates open connectivity and vendor equipment interoperability. The original version of the OPC specification, referred to as OPC classic, was implemented using Microsoft's COM/DCOM (Distributed Component Object Model) technology. In 2006, the OPC Foundation released a new standard, referred to as OPC Unified Architecture (UA), which does not use COM/DCOM. The known components of the identified Havex payload do not appear to target devices using the newer OPC UA standard.

Industrial Network Scanner

Another payload of interest is a network scanner module that was first reported by Kaspersky Lab. According to their report, this module's main functionality is to scan the local network and look for all hosts listening on ports related to industrial protocols.

Summary

ICS-CERT has published detailed information about the affected vendors, timelines of infection and an appendix of indicators to the US-CERT Secure Portal for critical infrastructure owners and operators. ICS-CERT recommends that organizations review these and other reports and leverage the indicators to look for signs of compromise within their business and control systems environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation. More specific and detailed mitigations can also be found at https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01.

REPORTING INCIDENTS

Sharing information about cyber incidents impacting your organization is essential to improving the overall security posture of our nation's critical infrastructure. We encourage critical infrastructure asset owners to contact ICS-CERT for assistance in responding to all cyber incidents impacting their business or control system environments. With our unique perspective and access to the breadth of knowledge available through our government and community partnerships, ICS-CERT is able to leverage that information to improve awareness and provide actionable information to the entire community without disclosing the identity or sensitive information about the reporting organization. ICS-CERT is also able to correlate the suspicious activity with other reported incidents, identify previous activity by the threat actor and share threat actor techniques and tactics with the reporting organization to assist with identifying the extent of intrusion and developing strategies for recovery. Incident information is also cataloged for future reference in responding to other emerging incidents and is protected from disclosure under Protected Critical Infrastructure Information (PCII) regulations.

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

ICS-CERT leverages the PCII Program to analyze and protect data about cyber incidents reported to DHS. The PCII Program was created by Congress through the Critical Infrastructure Information Act of 2002, ensuring that PCII in the government's hands is protected from disclosure. PCII is a key component in the effort to protect the Nation's critical infrastructure from cyber attacks and other risks.

Critical infrastructure partners can be confident that sharing their information with the government will not expose sensitive or proprietary data. PCII protection safeguards critical infrastructure information voluntarily shared with DHS. It ensures that the information will be used for homeland security purposes and cannot:

- Be disclosed through a Freedom of Information Act (FOIA) request or through a request under a similar state, tribal, or territorial disclosure law
- Be disclosed in civil litigation
- Be used for regulatory purposes.

Learn more about the PCII Program by visiting http://www.DHS.gov/PCII or email: pcii-info@dhs.gov.

For industrial control systems security information and incident reporting, please visit our web site at: http://ics-cert.us-cert.gov/.

ICS-CERT NEWS

PRESERVATION OF INFORMATION IS CRITICAL

So you think you've been compromised…now what? Preserving forensic data is an essential preliminary step in a sound incident response plan. Protecting and retaining valuable information in the wake of a cyber intrusion is crucial to your organization's ability to

identify the extent of an intrusion and develop a recovery plan. Organizations faced with the presence of malicious software or threat actors on their systems often do not know how to properly react. Whether organizations conduct their own response efforts or rely on services from a third party, it is important to understand that digital evidence can be fragile. Any action performed on the systems could result in changes to memory, files, or logs. Some of the most important forensic evidence can be found in fragile areas such as volatile memory or logs with retention restrictions. Two of the best sources for identifying compromised hosts are network logs and packets. Organizations should consider the following recommendations to ensure that this information is usable, trustworthy, and available in their environment:

- Consolidate network-level logging (network traffic information, DNS logs, firewall logs, network IDS logs, etc.) into a central repository that is backed up and protected from tampering
- Enable local system logging to provide a larger breadth of information available to forensic analysts
- Lengthen the retention period of this type of data by providing adequate storage space and access as well as promoting appropriate corporate data policies.

After identifying a system that is suspected of being compromised, responders should be careful about making any changes to the system. While some changes may be obvious, such as the installation of new programs or applications, others are less so. Organizations that are suspicious a host system may be compromised should follow these recommendations:

- **Do not turn off the system** - Turning off the system will result in lost forensic memory artifacts. When a computer is turned off, it initiates a series of commands that make changes to the hard drive and result in the loss of volatile data stored in registries, cache and random access memory (RAM).
- **Do not immediately disconnect from the network** - Disconnecting from the network before imaging system memory and hard drives can tip off an attacker and result in the loss of malware and indicators needed for a successful response. At the same time, staying connected to the network could continue to expose the victim to data exfiltration and lateral movement of the attacker. Responders are encouraged to weigh the costs and benefits of either action before committing to a decision.
- **Do not run antivirus programs** - The use of antivirus products on a system can be invasive because they access virtually every file on the system. This can cause file last-access times to change, system logs to roll over, and add additional data points that must then be analyzed by the forensic investigator.
- **Do not run any registry or file cleaner programs** - Similar to antivirus programs, these programs destroy forensic artifacts in the registry and memory that are useful for forensic analysis.
- **Do not install or run any additional tools** - By running or installing programs, changes are made to the system, which result in forensic data loss. The exception to this rule would be running programs necessary to image the system.

So where should you start? Prior to taking any other actions to respond to a suspected compromise, organizations should first take an image of the suspect computer's memory and drive. Because the memory is volatile, the memory image should be taken first. The memory image and the hard drive image are bit-by-bit copies of the original. In addition, because images can fail, groups should collect two clones, one for analysis and one as a backup. Any analysis of the system is conducted on the backup images to preserve the state of the originals.

When a suspected compromise occurs, it is of utmost importance to preserve any forensic data that exist on the system memory. It is important to keep logs of the system as well as react in a manner that does not destroy evidence when a compromise is suspected. When an organization reacts quickly and preserves forensic information, the likelihood of identifying the nature of the infection increases, and the ability to implement defenses for the future improves.

ASSESSMENT SERVICE OFFERINGS

The ICS-CERT assists critical infrastructure asset owners in protecting their control systems and networks against cyber threats through our no-cost assessment offerings. The program provides three types of voluntary cybersecurity assessments: a Cyber Security Evaluation Tool (CSET®) review, a Design Architecture Review (DAR) and a Network Architecture Verification and Validation (NAVV) review.

The CSET exists as a downloadable application (free of charge), which can be installed locally on a standalone workstation or laptop (https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET). ICS-CERT provides facilitated CSET services for asset owners, where the team will guide an asset owner through a step-by-step process to assess their environment, based on a series of questions derived from industry recognized standards, guidelines and best practices. The process helps asset owners create a snapshot of their cybersecurity posture and provides them with a mechanism to assess cybersecurity strengths and weaknesses within their control system environments.

A DAR is a "deep-dive" network architecture review and analysis that includes a comprehensive evaluation and discovery process, focusing on defense-in-depth strategies encompassing an asset owner's network perimeter defenses, zoning and network segmentation controls, and the communication flows occurring both within and to/from the control systems network. A DAR provides asset owners with a robust evaluation of their system interdependencies and vulnerabilities and with specific mitigation options.

A NAVV review encompasses network traffic analysis within a control systems environment. The analysis identifies device-to-device communications and correlates all the networked components within the ICS network. This provides the asset owners with an accurate view of their environment, which can then be compared to their design architecture in order to verify approved communications. This review provides additional value for an asset owner, including:

- Verifying the accuracy of the ICS network topology diagrams
- Identifying any potential rogue devices or malicious data communications
- Analyzing data flows to ensure that boundary protection devices are working as designed
- Identifying opportunities or areas for improving zoning and perimeter protections
- Base lining the ICS network
- Training on how to passively scan ICS networks.

Previously conducted NAVV's have identified out-of-band communications, misconfigured systems, rogue devices (including undefined communications) and devices attempting to initiate external communication requests to systems outside of the defined ICS perimeter.

ICS-CERT conducted 53 onsite assessments from May to August, 2014. Table 1 lists these assessments by sector, and Table 2 lists the assessments by type.

Table 1. Assessments by sector May – August, FY 2014.

Assessments by Sector	Fiscal (FY) Year 2014				May – August Totals
	May	June	July	August	
Chemical				1	1
Commercial Facilities					
Critical Manufacturing					
Dams					
Defense Industrial Base					
Emergency Services					
Energy	4		26	2	32
Finance Services					
Food & Agriculture					
Government Facilities				1	1
Healthcare & Public Health					
Information Technology					
Nuclear Reactors, Materials & Waste	1				1
Telecommunication					
Transportation	1	2			3
Water & Wastewater Systems	1	3	7	4	15
Monthly Totals	**7**	**5**	**33**	**8**	**53 Total Assessments**

Table 2. Assessments by type May – August, FY 2014.

Assessments by Type	Fiscal (FY) Year 2014				May – August Totals
	May	June	July	August	
CSET	4	4	7	2	17
DAR	2	1	16	4	23
MIR	1				1
NAVV			10	2	12
Monthly Totals	**7**	**5**	**33**	**8**	**53 Total Assessments**

ICS-CERT performed 418 onsite assessments from 2009 to August 31, 2014. Figure 1 represents the total number of CSET, DAR and NAVV assessments that were completed, by location. Table 3 shows the total number of assessments listed by sector.

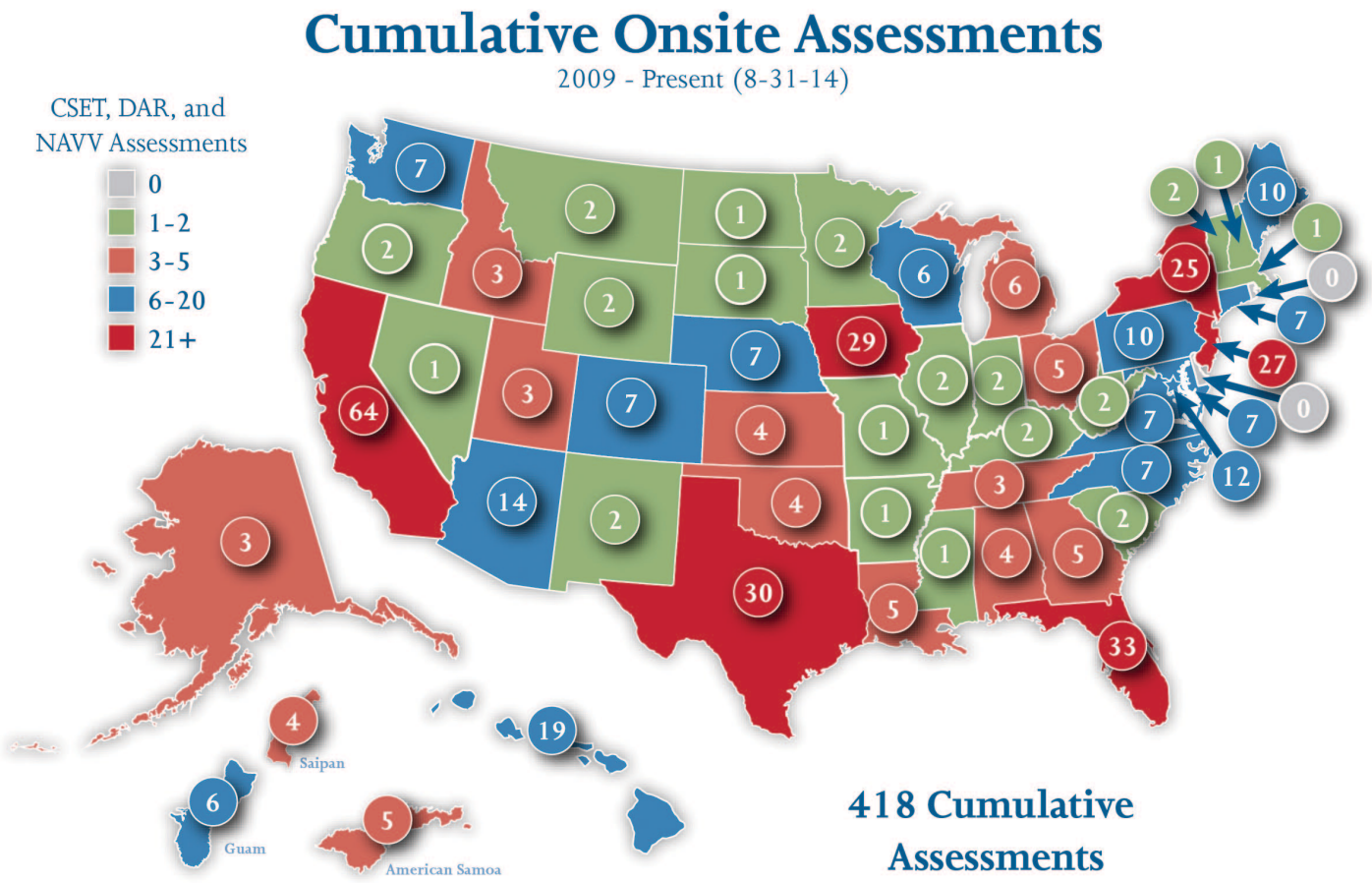

Figure 1. Map breakout of cumulative onsite assessments, 2009 through August 2014.

Table 3. Total ICS-CERT assessments by fiscal year and sector, 2009 – August 31, 2014.

Sector	Fiscal (FY) Year Assessments						May – August Totals
	2009	2010	2011	2012	2013	2014	
Chemical		3	1	4		1	**9**
Commercial Facilities	1		8	2			**11**
Communications			2		2		**4**
Critical Manufacturing		2	4	1			**7**
Dams		1					**1**
Defense Industrial Base	1	1		12	1		**15**
Emergency Services			2	5			**7**
Energy	2	12	10	7	19	43	**93**
Financial Services		2	1	6			**9**
Food & Agriculture		0	5				**5**
Government Facilities	1	6	7	2	2	5	**23**
Healthcare & Public Health	2	5	7		5		**19**
Information Technology	1		3	3	2		**9**
Nuclear Reactors, Materials & Waste			1	7	8	3	**19**
Transportation Systems	2	5	9	13	10	10	**49**
Water & Wastewater Systems	10	20	21	27	23	37	**138**
Total by Year / Cumulative	**20**	**57**	**81**	**89**	**72**	**99**	**418**

Over time, ICS-CERT has noted a positive trend of asset owners and operators gradually improving and enhancing the cybersecurity posture of their ICS infrastructure. Although the trend is moving in a positive direction, cybersecurity gaps still remain and should be addressed in order to reduce the risk of cyber threats.

Table 4 lists the common industry vulnerabilities and weaknesses identified in 2013 (through both onsite DAR and NAVV assessments). The most common weaknesses, observed on a repeated basis, encompassed a lack of zoning and segmentation, along with deficiencies in perimeter protections for ICS enclaves and network zones.

Zoning/Network Segmentation

An ICS cybersecurity posture can be bolstered significantly by creating zones as data pass between trusted and untrusted areas and from one physical area to another. Zoning encompasses three of the most common vulnerabilities identified by DAR and NAVV assessments: perimeter defense, ICS internal zoning, and boundary protections.

Zoning is a critical security measure to protect critical services, data, processes, and communication channels from manipulation and theft. Based on the concept of zones and cybersecurity protections, it is recommended that firewalls and IDSs be utilized at remote locations.

ICS internal zoning includes critical boundary protections that need to be considered as a first line of defense from untrusted networks. Internal protections are also critical when untrusted communication lines are used to interconnect a wide area network (WAN) environment to a control system network.

Table 4. Common vulnerabilities identified by 2013 onsite DAR and NAVV assessments.

Category		Common Vulnerabilities
Zoning	Perimeter Defense And Boundary Protections	Systems providing a dual-homed capability - bridging an ICS enclave to the corporate network infrastructure (bypassing perimeter defenses)
		Flat networks – no segmentation or perimeter protections between the ICS and corporate network environments
	ICS Internal Zoning	No firewall protections between independent control centers
		No DMZ segmenting the ICS and corporate networks
		External VPN access to the corporate environment, providing access to the ICS environment (because of a lack of zoning or network segmentation)
		Remote Desktop into the ICS environment from untrusted network segments
		Single Historian (DB) shared between zones (ICS & corporate)
	Boundary Protections	Lack of adequate firewall protections between zones
		Minimal firewall rule sets (providing a large scope of access to/from the ICS segment)
		No egress filtering or monitoring for data flows originating from within the ICS network segment
		Lack of auditing or verification of existing firewall rules (or security device configurations)
Remote Access		Modem banks configured for auto-answer
		No two factor authentication for remote access
		Outbound internet connections – which bypass security/screening appliances
Authentication		Shared system user accounts
		ICS auto logon (for systems within unmanaged or unsecured areas)
		Simple single sign-on passwords
		Limited port security on Layer 2 network devices with no MAC filtering
Media Protections		Usage of the same engineering workstations and laptops on both corporate and ICS networks
		No restricted use of digital media
		No disk encryption
Monitoring		No intrusion detection systems (IDSs)
		Improper placement of IDS (which may be blinded to detecting attacks that occur over encrypted or out-of-band communication channels)
		No base lining of data and traffic flows within the ICS environment
		Lack of egress monitoring/filtering
		Logging (including archiving) of events occurring within the ICS enclave

Boundary Protections

Boundary protections create a layered defensive strategy that bolsters an entity's ability to thwart cyber threats. Dividing common control systems architecture into zones can assist organizations in creating logical boundaries in order to effectively apply multiple layers of defense.

Remote access

Remote access has been identified as a primary entry point for attacks. When remote access is not properly designed, it can be a huge vulnerability by providing an attacker with unabated access from an untrusted network directly to a control system device. In addition, remote access creates a potentially vulnerable extension of the ICS network boundary and perimeter. A best

practice for remote access is to use a VPN tunnel to connect to an administrative system within a managed and restricted security zone (DMZ).

Summary

Setting priorities for cybersecurity and developing a risk-based approach for identifying threats, vulnerabilities, and associated consequences is crucial for ICS asset owners. As cybersecurity threats have evolved and attacks have increased, cybersecurity for ICS asset owners has become a necessity for basic operation; it is even more important for successful and optimal business performance.

As ICS communication technology continues to grow in importance, it is imperative for individual asset owners to make the needed investments in cybersecurity to fully protect the nation's critical infrastructure from cyber threats.

WEB-BASED TRAINING IS NOW AVAILABLE

Training is an important offering conducted by the ICS-CERT program. The program recently adopted a blended learning approach to enhance the training opportunities offered by the program. A new Introduction to ICS Cybersecurity course blends web-based and instructor-led methods. The curriculum is made up of ten modules and is available online at no cost.

The challenge solved by this new approach was three-fold. First, trainees have asked for materials in a format that is more efficient to access. Web-based training allows for trainees to access the course on their own time, in a setting that allows for asynchronous interaction, and is self-paced to better fit trainees' work schedules.

The second challenge was to reduce redundancy in the training materials. As the ICS-CERT cybersecurity training program has matured and developed course materials to support its growth, the courses were designed to build on each other. Ideally, a trainee will take the Introduction to ICS Cybersecurity course, followed by Intermediate Level courses, eventually completing the Technical Level ICS Cybersecurity Training. However, the program doesn't require prerequisites for attending the courses. As a result, trainees with different knowledge levels are completing the courses.

The online courses bridge the gap between trainees encountering redundant materials during higher-level classes and others being unprepared by offering advanced materials. Remedial information has also been removed from the advanced courses to ensure the curriculum is properly aligned to the course level.

Another opportunity for trainees to ensure that they are prepared for the advanced trainings is through a test-out option. Throughout this fiscal year, test-out options will become available for all the modules. Trainees well versed in an area will have the option to test-out of the modules, allowing them to focus on the topics that are of greatest importance to them.

The final challenge addressed by creating online training was the travel required for training. Prior to the online training courses, trainees were required to locate and then attend the ICS-CERT Cybersecurity training in person. Web-based courses alleviate the time, cost and inconvenience of traveling to attend multiple in person sessions.

In addition to blending methods and creating web-based modules, the program employs a learning management system (LMS). The LMS is a software application for the administration, documentation, tracking, reporting and delivery of training courses. The trainee benefits of this service are as follows:

- Supports the creation of a unique user id and provides credit for course completion
- Provides training courses using varied multimedia approaches (videos, audio, PowerPoint, Flash)
- Facilitates interoperability between eLearning software products through Supports Sharable Content Object Reference Model (SCORM) compliance for web-based training courses
- Enables live training events, training invitations, self-registration and attendance tracking
- Assists in tracking, analyzing and reporting course statistics
- Ensures course availability on mobile device (iPads, iPhones or Android devices) or desktop.

Last quarter, over 3,700 trainees initiated online training with over 400 of those completing their selected courses. Trainees are accessing the courses from several states and countries. You may view this web-based training at: https://ics-cert-training.inl.gov/.

ICSJWG SPRING MEETING RECAP

The Industrial Control Systems Joint Working Group (ICSJWG) 2014 Spring Meeting was held in Indianapolis, Indiana, and was attended by approximately 220 attendees composed of asset owners and operators, government professionals, vendors, systems integrators and academic professionals from around the globe.

Key highlights from the meeting were an opening keynote presentation by Indiana Governor Mike Pence, as well as two more keynote presentations from the Office of Cybersecurity and Communications: Gregory Touhill, Deputy Assistant Secretary for Cybersecurity Operations and Programs; and Larry Zelvin, Director of the National Cybersecurity and Communications Integration Center. Other participants and researchers provided a variety of presentations to include demos and lightning round talks,

which offered the opportunity for attendees to discuss the latest initiatives impacting the security of industrial control systems and the risk of threats and vulnerabilities to these systems.

ICSJWG FALL MEETING

The next ICSJWG event will be October 7−9, 2014, in Idaho Falls, Idaho. The 2014 Fall ICSJWG Meeting will bring together asset owners and operators, government professionals, vendors, systems integrators and academic professionals to discuss the latest initiatives impacting security of our critical infrastructure and interact with peers addressing the risk of threats and vulnerabilities to their systems.

ICSJWG 2014 Fall Meeting
October 7−9, 2014
Energy Innovation Laboratory,
775 University Boulevard,
Idaho Falls, Idaho, USA

The meeting will include discussions about security of industrial controls and critical infrastructure. We will include keynote speakers, practical demonstrations, plenary sessions, panel presentations and lightning rounds, as well as classified and unclassified briefings. We are also planning tours of relevant facilities across the Idaho National Laboratory campus to take advantage of the location at a leading edge national lab.

More information about the meeting will be sent out as these special events are finalized.

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.

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-14-176-02A ICS Focused Malware (Update A), 06/27/2014

ICS-ALERT-14-155-01A Daktronics Vanguard Default Credentials, 06/05/2014

ICS-ALERT-14-099-01E Situational Awareness Alert for OpenSSL Vulnerability, 04/29/2014

ADVISORIES

ICSA-14-238-01 CG Automation Improper Input Validation, 08/26/2014

ICSA-14-238-02 Schneider Electric Wonderware Vulnerabilities, 08/26/2014

ICSA-14-198-03C Siemens OpenSSL Vulnerabilities, 08/21/2014

ICSA-14-226-01 Siemens SIMATIC S7-1500 CPU Denial of Service, 08/14/2014

ICSA-14-196-01 SubSTATION Server Telegyr 8979 Master Vulnerabilities, 07/31/2014

ICSA-14-189-02 Innominate mGuard Unauthorized Leakage of System Data, 07/29/2014

ICSA-14-205-01 Morpho Itemiser 3 Hard-Coded Credential, 07/24/2014

ICSA-14-205-02 Siemens SIMATIC WinCC Vulnerabilities, 07/24/2014

ICSA-14-007-01B Sierra Wireless AirLink Raven X EV-DO Vulnerabilities, 07/23/2014

RECENT PRODUCT RELEASES - Continued

ADVISORIES

ICSA-14-203-01 Omron NS Series HMI Vulnerabilities, 07/22/2014

ICSA-14-175-01 Honeywell FALCON XLWeb Controllers Vulnerabilities, 07/22/2014

ICSA-14-202-01 OleumTech WIO Family Vulnerabilities, 07/21/2014

ICSA-14-198-01 Cogent DataHub Code Injection Vulnerability, 07/17/2014

ICSA-14-198-02 Advantech WebAccess Vulnerabilities, 07/17/2014

ICSA-14-189-01 Yokogawa Centum Buffer Overflow Vulnerability, 07/08/2014

ICSA-14-126-01A ABB Relion 650 Series OpenSSL Vulnerability (Update A), 07/08/2014

ICSA-14-178-01 ICS Focused Malware, 06/30/2014

ICSA-14-156-01 OpenSSL Releases Security Advisory, 06/05/2014

ICSA-14-154-01 COPA-DATA Improper Input Validation, 06/03/2014

ICSA-14-149-01 Triangle MicroWorks Uncontrolled Resource Consumption, 05/29/2014

ICSA-14-149-02 Cogent DataHub Vulnerabilities, 05/29/2014

ICSA-14-087-01A Siemens ROS Improper Input Validation, 05/27/2014

ICSA-14-051-03B Siemens RuggedCom Uncontrolled Resource Consumption Vulnerability, 05/27/2014

ICSA-14-133-02 Emerson DeltaV Vulnerabilities, 05/22/2014

ICSA-14-105-03B Siemens Industrial Products OpenSSL Heartbleed Vulnerability, 05/20/2014

ICSA-14-135-01 CSWorks Software SQL Injection Vulnerability, 05/15/2014

ICSA-14-135-02 Schneider Electric Wonderware Intelligence Security Patch for OpenSSL Vulnerability, 05/15/2014

ICSA-14-135-03 Siemens RuggedCom ROX-based Devices Certificate Verification Vulnerability, 05/15/2014

ICSA-14-135-04 Unified Automation OPC SDK OpenSSL Vulnerability, 05/15/2014

ICSA-14-135-05 OpenSSL Vulnerability, 05/15/2014

ICSA-14-133-01 Yokogawa Multiple Products Vulnerabilities, 05/13/2014

ICSA-14-070-01A Yokogawa CENTUM CS 3000 Vulnerabilities, 05/13/2014

ICSA-14-128-01 Digi International OpenSSL Vulnerability, 05/08/2014

ICSA-14-126-01 ABB Relion 650 Series OpenSSL Vulnerability, 05/06/2014

ICSA-14-121-01 AMTELCO miSecure Vulnerabilities, 05/01/2014

ICSA-14-091-01 Ecava IntegraXor Guest Account Information Disclosure Vulnerability, 04/29/2014

ICSA-14-114-01 Certec atvise scada OpenSSL Heartbleed Vulnerability, 04/24/2014

ICSA-14-114-02 Siemens SIMATIC S7-1200 CPU Web Vulnerabilities, 04/24/2014

ICSA-14-084-01 Festo CECX-X-(C1/M1) Controller Vulnerabilities, 04/24/2014

ICSA-14-107-02 InduSoft Web Studio Directory Traversal Vulnerability, 04/24/2014

ICSA-14-107-01 Siemens SINEMA Vulnerabilities, 04/17/2014

ICSA-14-105-02A Innominate mGuard OpenSSL HeartBleed Vulnerability, 04/17/2014

ICSA-14-105-01 Progea Movicon SCADA Information Disclosure Vulnerability, 04/15/2014

ICSA-14-100-01 IOServer Out of Bounds Read Vulnerability, 04/10/2014

RECENT PRODUCT RELEASES - Continued

ICSA-12-342-01B Rockwell Allen-Bradley MicroLogix, SLC 500, and PLC-5 Fault Generation Vulnerability, 04/10/2014

ICSA-13-291-01B DNP3 Implementation Vulnerability, 04/09/2014

ICSA-14-098-01 OSISoft PI Interface for DNP3 Improper Input Validation, 04/08/2014

ICSA-14-098-02 WellinTech KingSCADA Stack-Based Buffer Overflow, 04/08/2014

ICSA-14-098-03 Siemens Ruggedcom WIN Products BEAST Attack Vulnerability, 04/08/2014

ICSA-14-079-03 Advantech WebAccess Vulnerabilities, 04/08/2014

ICSA-14-093-01 Schneider Electric OPC Factory Server Buffer Overflow, 04/03/2014

ICSA-14-086-01A Schneider Electric Serial Modbus Driver Buffer Overflow, 04/01/2014

OTHER

January-April 2014–ICS-CERT Monitor

Follow ICS-CERT on Twitter: @icscert

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Researchers find it's terrifyingly easy to hack traffic lights
2014-08-20
http://arstechnica.com/security/2014/08/researchers-find-its-terrifyingly-easy-to-hack-traffic-lights/

Nuke Regulator Hacked by Suspected Foreign Powers
2014-08-18
http://www.nextgov.com/cybersecurity/2014/08/exclusive-nuke-regulator-hacked-suspected-foreign-powers/91643

As Stuxnet Anniversary Approaches, New SCADA Attack Is Discovered
2014-07-26
http://www.darkreading.com/as-stuxnet-anniversary-approaches-new-scada-attack-is-discovered/d/d-id/1278881

Cyber threats put energy sector on red alert
2014-07-15
http://thehill.com/policy/energy-environment/212220-cyber-threats-put-energy-sector-on-red-alert

70% of Critical Infrastructure Organizations Suffered Breaches in the Last Year
2014-07-11
http://www.infosecurity-magazine.com/view/39281/70-of-critical-infrastructure-organizations-suffered-breaches-in-the-last-year/

Motives Behind HAVEX ICS Malware Campaign Remain a Mystery
2014-07-07
http://threatpost.com/motives-behind-havex-ics-malware-campaign-remain-a-mystery

ICS-CERT sounds alarm on critical infrastructure attacks
2014-07-02
http://fcw.com/articles/2014/07/02/dhs-warning-critical-infrastructure-attacks.aspx

OpenSSL revived with survival roadmap
2014-07-01
http://www.theregister.co.uk/2014/07/01/openssl_roadmap/
https://www.openssl.org/about/roadmap.html

Energy providers hacked through malicious software updates
2014-06-30
http://www.pcworld.com/article/2449680/energy-providers-hacked-through-malicious-software-updates.html
http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia html
http://www.bloomberg.com/news/2014-06-30/symantec-warns-energetic-bear-hackers-threaten-energy-firms html
http://www.washingtonpost.com/news/morning-mix/wp/2014/07/01/reports-reveal-ongoing-cyberattacks-on-u-s-and-european-energy-sector/
http://blogs.wsj.com/digits/2014/06/30/top-u-k-cyber-cop-russian-hackers-are-our-biggest-threat/

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

Russian Hackers Targeting Oil and Gas Companies
2014-06-30
http://www nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html

Active malware operation let attackers sabotage US energy industry
2014-06-30
http://arstechnica.com/security/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/

Dragonfly: Western Energy Companies Under Sabotage Threat
2014-06-30
http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

New Oil and Natural Gas ISAC Launches
2014-06-27
http://threatpost.com/new-oil-and-natural-gas-isac-launches/106902

Montana Health Department Hacked
2014-06-25
http://www.informationweek.com/healthcare/security-and-privacy/montana-health-department-hacked/d/d-id/1278872

Response on Today's FERC Orders
2014-06-19
http://www nerc.com/news/Pages/Response-on-Today%27s-FERC-Orders.aspx

FireEye / Mandiant Try The ICS Market
2014-06-18
http://www.digitalbond.com/blog/2014/06/18/fireeye-mandiant-try-the-ics-market/

Control System Visualization – A Military View
2014-06-11
http://chemical-facility-security-news.blogspot.com/2014/06/control-system-visualization-military.html

SP 800-82 Rev.2 DRAFT Guide to Industrial Control Systems (ICS) Security NIST SP 800-82 Rev. 2
2014-05-14
http://csrc nist.gov/publications/PubsDrafts.html#SP-800-82-Rev.2
http://csrc nist.gov/publications/drafts/800-82r2/sp800_82_r2_draft.pdf

DOE issues guidance on electric grid cybersecurity
2014-04-28
http://thehill.com/policy/energy-environment/204544-doe-issues-guidance-on-electric-grid-cybersecurity
http://energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain

What Heartbleed Means for Critical Infrastructure
2014-04-23
http://www forbes.com/sites/thebakersinstitute/2014/04/23/what-heartbleed-means-for-critical-infrastructure-2/

DHS Encourages Guarding Oilfield Against Cyber Threats
2014-04-23
http://www.govtech.com/security/DHS-Encourages-Guarding-Oilfield-Against-Cyber-Threats html

Government, Industry Target Air Traffic Cyber Attacks
2014-04-25
http://www federaltimes.com/article/20140425/CYBER/304250012/Government-industry-target-air-traffic-cyber-attacks

Inside the Ring: U.S. Power Grid Defenseless From Physical and Cyber Attacks
2014-04-16
http://www.washingtontimes.com/news/2014/apr/16/inside-the-ring-us-power-grid-defenseless-from-att/

Cyber Threat Moving to Critical Infrastructure, Study Shows
2014-04-09
http://www.computerweekly.com/news/2240217851/Cyber-threat-moving-to-critical-infrastructure-study-shows

Willis Insurance Predicts Energy Cyber-Attack 'Catastrophe' Ahead
2014-04-08
http://www forbes.com/sites/davidnicholson/2014/04/08/willis-insurance-predicts-energy-cyber-attack-catastrophe-ahead/
http://www reuters.com/article/2014/04/08/energy-cybercrime-idUSL6N0N02CR20140408

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

Small-Scale Power Grid Attack Could Cause Nationwide Blackout, Study Says
2014-03-13
http://www foxnews.com/politics/2014/03/13/us-risks-national-blackout-from-power-grid-attack-study-says/

http://online.wsj.com/news/articles/SB10001424052702304020104579433670284061220

Feds To Improve Threat Information Sharing
2014-03-31
http://www.informationweek.com/government/cybersecurity/feds-to-improve-threat-information-sharing/d/d-id/1141598

UPCOMING EVENTS

October

ICSJWG 2014 Fall Meeting Industrial Control Systems Joint Working Group (ICSJWG)

October 7–9, 2014
Idaho Falls, Idaho, USA

Registration

October

Cybersecurity Training for Industrial Control Systems (Regional Event, 4 days)

October 20–23, 2014
Houston, Texas

Course Description and Registration

December

Industrial Control Systems Cybersecurity (301) Training (5 days) North American Partners

November 8–12, 2014
Idaho Falls, Idaho, USA

Course Description and Registration

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.

COORDINATED VULNERABILITY DISCLOSURE - Continued

RESEARCHERS ASSISTING ICS-CERT WITH PRODUCTS THAT WERE PUBLISHED MAY/JUNE

ICS-CERT appreciates having worked with the following researchers:

- Adam Crain of Automatak and Chris Sistrunk of Mandiant, ICSA-14-238-01 CG Automation Improper Input Validation, 08/26/2014.
- Timur Yunusov, Ilya Karpov, Sergey Gordeychik, Alexey Osipov, and Dmitry Serebryannikov of the Positive Technologies Research Team, ICSA-14-238-02 Schneider Electric Wonderware Vulnerabilities, 08/26/2014.
- Arnaud Ebalard from Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), ICSA-14-226-01 Siemens SIMATIC S7-1500 CPU Denial of Service, 08/14/2014.
- Adam Crain of Automatak and Chris Sistrunk of Mandiant, ICSA-14-196-01 SubSTATION Server Telegyr 8979 Master Vulnerabilities, 07/31/2014.
- The Applied Risk Research team, ICSA-14-189-02 Innominate mGuard Unauthorized Leakage of System Data, 07/29/2014.
- Independent researchers Billy Rios and Terry McCorkle, ICSA-14-205-01 Morpho Itemiser 3 Hard-Coded Credential, 07/24/2014.
- Researchers Sergey Gordeychik, Alexander Tlyapov, Dmitry Nagibin, and Gleb Gritsai of Positive Technologies, ICSA-14-205-02 Siemens SIMATIC WinCC Vulnerabilities, 07/24/2014.
- A researcher at Cimation, ICSA-14-007-01B Sierra Wireless AirLink Raven X EV-DO Vulnerabilities, 07/23/2014.
- Joel Sevilleja Febrer of S2 Grupo, ICSA-14-203-01 Omron NS Series HMI Vulnerabilities, 07/22/2014.
- Martin Jartelius of Outpost24 and Juan Francisco Bolivar, ICSA-14-175-01 Honeywell FALCON XLWeb Controllers Vulnerabilities, 07/22/2014.
- Lucas Apa and Carlos Mario Penagos Hollman of IOActive, ICSA-14-202-01 OleumTech WIO Family Vulnerabilities, 07/21/2014.
- Security researcher John Leitch and Zero Day Initiative (ZDI), ICSA-14-198-01 Yokogawa Centum Buffer Overflow Vulnerability Cogent DataHub Code Injection Vulnerability, 07/17/2014.
- ZDI, ICSA-14-198-02 Advantech WebAccess Vulnerabilities, 07/17/2014.
- Researcher group Rapid7, ICSA-14-189-01 Yokogawa Centum Buffer Overflow Vulnerability, 07/08/2014.
- KIKUCHI Masashi of Lepidum Co. Ltd., Imre Rad of Search-Lab Ltd., Jüri Aedla, Felix Gröbert, and Ivan Fratrić at Google, ICSA-14-156-01 OpenSSL Releases Security Advisory, 06/05/2014.
- Adam Crain of Automatak and Chris Sistrunk of Mandiant, ICSA-14-154-01 COPA-DATA Improper Input Validation, 06/03/2014.
- Adam Crain of Automatak and Chris Sistrunk of Mandiant, ICSA-14-149-01 Triangle MicroWorks Uncontrolled Resource Consumption, 05/29/2014.
- Independent researcher Alain Homewood, ICSA-14-149-02 Cogent DataHub Vulnerabilities, 05/29/2014.
- Researcher Aivar Liimets from Martem Telecontrol Systems, ICSA-14-087-01A Siemens ROS Improper Input Validation, 05/27/2014.
- Researchers Ling Toh Koh, Ng Yi Teng, Seyed Dawood Sajjadi Torshizi, Ryan Lee, and Ho Ping Hou of EV-Dynamic, Malaysia, ICSA-14-051-03B Siemens RuggedCom Uncontrolled Resource Consumption Vulnerability, 05/27/2014.
- Kirill Nesterov, Alexander Tlyapov, Dmitry Nagibin, Alexey Osipov, and Timur Yunusov of Positive Technologies, ICSA-14-133-02 Emerson DeltaV Vulnerabilities, 05/22/2014.
- Joel Langill of Infrastructure Defense Security Services, ICSA-14-105-03B Siemens Industrial Products OpenSSL Heartbleed Vulnerability, 05/20/2014.
- Researcher John Leitch, working with HP's Zero Day Initiative (ZDI), ICSA-14-135-01 CSWorks Software SQL Injection Vulnerability, 05/15/2014.

COORDINATED VULNERABILITY DISCLOSURE - Continued

- Neel Mehta of Google Security on April 1, 2014, and 2 days later by a team of security engineers Riku, Antti, and Matti at Codenomicon, ICSA-14-135-05 OpenSSL Vulnerability, 05/15/2014
- Juan Vazquez of Rapid7 Inc., and independent researcher Julian Vilas Diaz, ICSA-14-070-01A Yokogawa CENTUM CS 3000 Vulnerabilities, 05/13/2014.
- Researcher Jared Bird of Allina Health, ICSA-14-121-01 AMTELCO miSecure Vulnerabilities, 05/01/2014.
- Independent researcher Andrea Micalizzi, aka rgod, ICSA-14-091-01 Ecava IntegraXor Guest Account Information Disclosure Vulnerability, 04/29/2014.
- Researcher Bob Radvanovsky of Infracritical, ICSA-14-114-01 Certec atvise scada OpenSSL Heartbleed Vulnerability, 04/24/2014.
- Ralf Spenneberg, Hendrik Schwartke, and Maik Brüggemann from OpenSource Training, ICSA-14-114-02 Siemens SIMATIC S7-1200 CPU Web Vulnerabilities, 04/24/2014.
- K. Reid Wightman of IOActive, Inc., ICSA-14-084-01 Festo CECX-X-(C1/M1) Controller Vulnerabilities, 04/24/2014.
- Zero Day Initiative (ZDI), ICSA-14-107-02 InduSoft Web Studio Directory Traversal Vulnerability, 04/24/2014.
- Researcher Bob Radvanovsky of Infracritical, ICSA-14-105-02A Innominate mGuard OpenSSL HeartBleed Vulnerability, 04/17/2014.
- Celil Ünüver of SignalSEC Ltd., ICSA-14-105-01 Progea Movicon SCADA Information Disclosure Vulnerability, 04/15/2014.
- Chris Sistrunk of Mandiant and Adam Crain of Automatak, ICSA-14-100-01 IOServer Out of Bounds Read Vulnerability, 04/10/2014.
- Independent researcher Matthew Luallen of CYBATI, ICSA-12-342-01B Rockwell Allen-Bradley MicroLogix, SLC 500, and PLC-5 Fault Generation Vulnerability, 04/10/2014.
- Adam Crain of Automatak and Chris Sistrunk, Sr. Consultant for Mandiant, ICSA-13-291-01B DNP3 Implementation Vulnerability, 04/09/2014.
- Adam Crain of Automatak and Chris Sistrunk, Sr. Consultant for Mandiant, ICSA-14-098-01 OSISoft PI Interface for DNP3 Improper Input Validation, 04/08/2014.
- An anonymous researcher working with HP's Zero Day Initiative, ICSA-14-098-02 WellinTech King SCADA Stack-Based Buffer Overflow, 04/08/2014.
- Researchers working with HP's Zero Day Initiative (ZDI), Andrea Micalizzi, aka rgod, Tom Gallagher, and an independent anonymous researcher, ICSA-14-079-03 Advantech WebAccess Vulnerabilities, 04/08/2014.
- Researcher Wei Gao, formerly of IXIA, ICSA-14-093-01 Schneider Electric OPC Factory Server Buffer Overflow, 04/03/2014.
- Carsten Eiram of Risk-Based Security, ICSA-14-086-01A Schneider Electric Serial Modbus Driver Buffer Overflow, 04/01/2014.

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT

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

Adam Crain
Alain Homewood
Alexander Tlyapov
Alexey Osipov
Andrea Micalizzi
Arnaud Ebalard
Aivar Liimets
Billy Rios
Bob Radvanovsky
Carlos Mario Penagos Hollmann
Carsten Eiram
Cecil Unuver
Cesar Cerrudo
Chris Sistrunk
Dmitry Nagibin
Dmitry Serebryannikov
Eireann Leverett
Eric Forner`
Eric Wustrow
Gleb Gritsai
Ho Ping Hou
Ilya Karpov
Jared Bird
J. Alex Halderman
Joel Langill
Joel Sevilleja Febrer
John Leitch
Juan Vasquez
Kirill Nesterov
Ling Toh Koh
Lucas Apa
Martin Jartelius
Matthew Luallen
Neel Mehta
Ng Yi Teng
Ralf Spenneberg
Reid Wightman
Ryan Lee
Sergey Gordeychick
Seyed Dawood Sajjadi Torshizi
Shawn Merdinger
Stephen Dunlap
Terry McCorkle
Timur Yunusov
Wei Gao

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.