Homeland Security

ICS-CERT MONITOR

Contents

National Cybersecurity and Communications Integration Center

ICS-CERT

This is a publication of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT is a component of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT coordinates control systems-related security incidents and information sharing with federal agencies; state, local, tribal, and territorial governments; and control systems owners, operators, and vendors to reduce the risk of cyber attack against the Nation's critical infrastructure.

This issue and past issues of the ICS-CERT Monitor can be found here: https://ics-cert.us-cert.gov/monitors

Contact Information

For questions related to this report or to contact ICS-CERT:

NCCIC/ICS-CERT Operations Center
Toll Free: 1-877-776-7585
International: 1-208-526-0900
Email: ics-cert@hq.dhs.gov
Web site: http://ics-cert.us-cert.gov

Report an ICS incident to ICS-CERT

Report an ICS software vulnerability

Get information about reporting

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 to receive up-to-date alerts and advisories related to industrial control systems (ICS) cybersecurity. To request a portal account, send your name, telephone contact number, email address, and company affiliation to ics-cert@hq.dhs.gov.

Downloading PGP/GPG Keys

https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT_PGP_Pub_Key.asc

Incident Response Activity

Notable Incident

ICS-CERT recently worked with an industrial control system asset owner following a report of possible intrusion activity targeting the entity's network. The asset owner operates in the power and water sectors, providing both power and water to their local community. The company was receptive to working with ICS-CERT and ultimately requested that ICS-CERT come onsite to gather data and attempt to discover compromises on their network. ICS-CERT held a conference call with the entity to plan onsite incident response actions, request technical information, and establish expectations. On the call, ICS-CERT learned that the asset owner was in the process of merging its power and water networks, which had previously operated independently.

When the ICS-CERT incident response team arrived onsite, they first met with network engineers and top executives. At the request of the company, the team temporarily installed network security monitoring equipment, gathered host and network data, and examined ICS equipment to assess network integrity. Initial analysis spotted low-level malware throughout the water network, but found no indication of the same on the power network.

Next the team visited several sites essential to the entity's operations. One of these sites was the distribution/transmission control center, where the team met with personnel who oversee operations on the power side and manually collected information from the site's servers/HMI. While reviewing the network architecture of the distribution/transmission control center and the data capture, the team discovered a wireless router that the asset owner believed to be disconnected from the network. The wireless router was active and allowed for direct access into the control system environment.

The team also visited the water control center and a power substation to examine equipment. At the water control center, the team discovered a cellular modem connected to the main water switch. The local staff was unsure of its direct function, but it was later identified as a cellular modem that allowed for remote vendor access via a simple username and password. While analyzing the collected data, TeamViewer connections were discovered on high value hosts (IT operations computers, billing, finance, and badging) to foreign hosts. The team confirmed with local staff that these were not legitimate and the activity was blocked by the asset owner.

At the end of the visit, the team provided the asset owner with its initial findings, as well as an assortment of best practices/recommendations specific to their environment. The customer was receptive to ICS-CERT's recommendations and requested additional support in the coming months to review the architecture/cyber security posture of its proposed new network.

Onsite Assessments Summary

ICS-CERT Assessment Activity for January/February 2016

ICS-CERT conducts onsite cybersecurity assessments of industrial control systems (ICSs) to help strengthen the cybersecurity posture of critical infrastructure owners and operators and of ICS manufacturers. In January/February 2016, ICS-CERT conducted 18 onsite assessments across four sectors (Table 1). Of these 18 assessments, five were Cyber Security Evaluation Tool (CSET®) assessments, eight were Design Architecture Review (DAR) assessments, and five were Network Architecture Verification and Validation (NAVV) assessments (Table 2). For detailed information on ICS-CERT's CSET, DAR, and NAVV assessments, go to https://ics-cert.us-cert.gov/assessments.

Table 1: Assessments by sector, January/February 2016.

Assessments by Sector	January 2016	February 2016	January/February Totals
Chemical	4		4
Commercial Facilities			
Communications	2		2
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy			
Financial Services			
Food and Agriculture			
Government Facilities		5	5
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems		7	7
Monthly Totals	**6**	**12**	**18 Total Assessments**

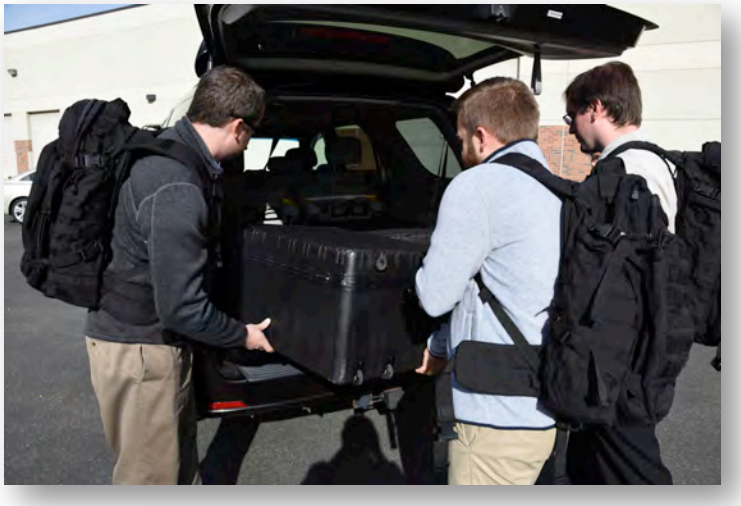
Table 2. Assessments by type, January/February 2016.

Assessments by Type	January 2016	February 2016	January/February Totals
CSET	2	3	5
DAR	3	5	8
NAVV	1	4	5
Monthly Totals	**6**	**12**	**18 Total Assessments**

Preparing for an Incident Response

Even with the best cyber defense mechanisms in place, cyber incidents will likely occur. Is your organization prepared to properly identify what went wrong and recover? Preparation and planning are essential to an organization's ability to respond to a cyber incident. The ability to identify the source of an incident and analyze the extent of the compromise is necessary to rapidly detect issues, minimize loss, mitigate exploited vulnerabilities, and restore computing services.

Cyber incidents are tense, complicated, and not often part of routine operations. When properly maintained, operational preparedness measures can ensure the availability of information necessary to recover from an incident quickly while minimizing the impact.



A dedicated incident handling team should be led by a senior technical staff member who has the authority to make key decisions in a timely manner. In addition to the lead and forensics analysts, a control systems incident response team should include control systems subject matter experts and stakeholders from corporate IT (both network and host management), public relations, legal counsel, and law enforcement, if necessary.

The team should be trained in proper incident handling techniques and should practice using the tools to establish and maintain proficiency. Control system environments have special needs that should be evaluated when establishing operating procedures. An overall incident preparedness checklist should be created and reviewed annually using a "table-top" exercise. Documentation should be accessible to operations personnel to help facilitate analysis of the incident and identify priorities for recovery. An incident response information gathering checklist should also be created. This checklist should identify the types of information that should be collected to aid analysis by external CERTs or partners.

It is also important to establish an "out-of-band" communications policy. Any communications regarding an incident or potential incident should not go through the standard communication channels, e.g., corporate email, VoIP systems, as these may already be compromised and will tip off the adversary that you are aware of their presence in your network. In addition, any files relating to the incident or handling policy should be stored off the network under the control of the incident response team.

Logging is an important aspect of incident response. System and network device logs are essential to incident investigators. The types of logging that should be considered include Firewall, Proxy, domain name server (DNS), dynamic host configuration protocol (DHCP), web app, audiovisual (A/V), intrusion detection system (IDS)/intrusion prevention system (IPS), and host and application logs. Additional logging to be considered is flow data from routers, switches, and packet captures. This type of network data will be helpful when responding to a control system event because network-related logs are sometimes all that is available. If the control system endpoints do support logging, these, too, should be reviewed for a better understanding of what took place. Log integrity is essential during an incident investigation; therefore, logs should be continuously stored on a separate system, frequently backed-up, and cryptographically hashed to allow detection of log alterations.

Other critical components of incident response are forensic data collection, analysis, and reporting. These elements are essential to preserving important evidence. Organizations should consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts. In addition, ICS-CERT subject matter experts are available to aid in incident response activities. Affected entities should not hesitate to contact ICS-CERT for assistance.

For additional information and resources on cyber incident response for industrial control systems, please see ICS-CERT's fact sheet titled Preparing for Incident Response. This fact sheet includes details on procedures, documentation, checklists, logging, and preserving forensic data. It also includes links to additional resources for developing incident response capabilities and plans. To report a cybersecurity incident to ICS-CERT, go here: https://ics-cert.us-cert.gov/Report-Incident.

ICS-CERT Releases CSET 7.1

ICS-CERT released the latest version of its Cyber Security Evaluation Tool (CSET), CSET 7.1, in February 2016. CSET provides a systematic, disciplined, and repeatable approach for evaluating an organization's cybersecurity posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to analyze their ICS and IT network security practices using many recognized government and industry standards and recommendations.

What's New?

- **NIST SP800-161.** This standard introduces supply chain management controls to CSET.
- **NERC CIP Compliance Risk Based Priority List.** Using the NERC CIP Violation Risk Factors, CSET 7.1 provides a priority ranked list of an asset owner's NERC-CIP controls based on assessment question answers and the assessor selection of questions or requirements.
- **Enhanced Dashboard.** The gaps analysis dashboard has been redesigned and now includes additional information and simplified navigation, improving access to detail charts.
- **Requirements organized according to standard.** When working with a single standard in the new CSET, users can see the questions and requirements presented in the order of the standard. Control identifiers are also based on the identifier used in the standard (e.g., AC-2) as opposed to arbitrary numbering. With this new version, users can perform text searches directly on the question screen, as well as sort and reorder questions based on how they apply to different standards.
- **Custom Parameter Values.** Users can now enter custom parameter values for standards with requirements that include parameters. Several standards allowed individual organizations to define their own time frequency or role definitions for some controls. These parameter values can be customized and stored in CSET 7.1.
- **Doubled Number of Network Components.** The number of network components has been doubled in Version 7.1. CSET 7.1 includes stencils for ICS, IT, medical, and emergency management radio components.

CSET is distributed freely to the public. For additional information on CSET or to download a copy, go to https://www.us-cert.gov/forms/csetiso assessments. To report a problem or request a new feature, go to http://cset.inl.gov.

ICS-CERT at the S4 Conference

In January, ICS-CERT attended Digital Bond's S4x16 ICS Security Conference in Miami. The S4 conference is a "SCADA and ICS security conference for people who want to see advanced ideas and technical content." The conference drew many of the top names in the industry to the stage, including keynote speaker General Michael Hayden.

The S4 main stage hosted the keynotes and presentations covering ICS vulnerabilities, responsible disclosure, threat intelligence, regulation, current events, and the electric grid, as well as many others. Stage 2 hosted more advanced technical content. This stage hosted presentations on monitoring ICS devices, forensics, detection, medical devices, and CANBUS.

With over 300 in attendance, ICS-CERT had the opportunity to meet with fellow researchers, catch up on the latest security trends and developments, make new connections, and coordinate any unanticipated vulnerability disclosures. ICS-CERT met with several vendors to continue building working relationships and foster collaboration. Several CERTS from around the world were in attendance, and ICS-CERT took the opportunity to meet and continue to increase ICS-CERT's international coordination capabilities.

ICS-CERT values its ability to collaborate at conferences like S4. The community engagement and situational awareness it provides furthers ICS-CERT's mission to reduce risk to the Nation's critical infrastructure by strengthening control systems security and resilience through public-private partnerships.

ICS-CERT Welcomes You to GovDelivery

You may have noticed that you are no longer receiving US-CERT Portal notifications for ICS-CERT publicly released alerts and advisories. That is because ICS-CERT recently launched a new digital subscription system with GovDelivery to continue to help you stay informed. By signing up for GovDelivery, you can receive new ICS-CERT product release notices directly to your inbox. Learn more, and sign up for GovDelivery here: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new

Industrial Control Systems Joint Working Group Meetings

ICS-CERT and the Industrial Control Systems Joint Working Group (ICSJWG) invite you to the ICSJWG 2016 Spring Meeting taking place at Chaparral Suites – Scottsdale (Soon to be Embassy Suites – Scottsdale) in Scottsdale, Arizona, on May 3–5. ICSJWG meetings provide a forum for all critical infrastructure (CI) stakeholders to gather and exchange ideas about critical issues in ICS cybersecurity. ICSJWG Meetings include keynote and breakout presentations, panels, demonstrations, a vendor expo, and networking opportunities. Each meeting is offered at no cost to attendees and is open to all who are interested.

Confirmed Keynote Speakers:

- Mark Fabro, President & Chief Security Scientist, Lofty Perch
- Frank Grimmelmann, President & CEO/Intelligence Liaison Officer, ACTRA

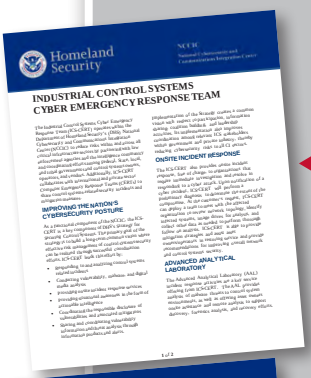
Meeting Highlights:

- Three full days of presentations
- ICSJWG's Vendor Expo
- "Ask Me Anything" session with NCCIC/ICS-CERT representatives
- International break-out/networking session
- Lightning Round presentations

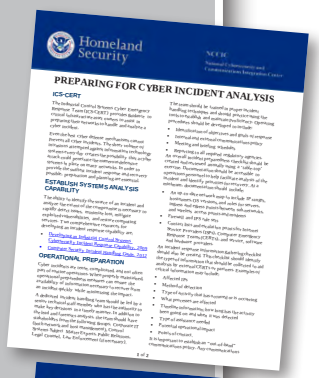
For additional information about the ICSJWG 2016 Spring Meeting, including registration and logistical details, please visit https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG or contact the ICSJWG Program Management Office at ICSJWG.Communications@hq.dhs.gov.

ICS-CERT Fact Sheets

ICS-CERT recently published eight updated fact sheets. To find the fact sheets online, click on the links below, or go to https://ics-cert.us-cert.gov/Information-Products and clink on the Fact Sheets tab.



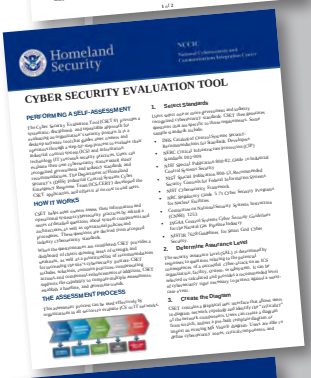
1. Industrial Control Systems Cyber Emergency Response Team



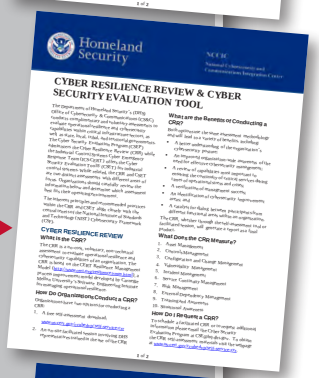
2. Preparing for Cyber Incident Analysis

3. Industrial Control Systems Joint Working Group

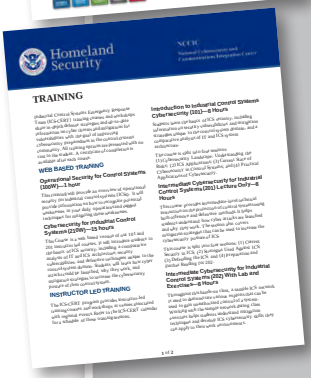
4. Control Systems Architecture Analysis Services



5. Cyber Security Evaluation Tool



6. Cyber Resilience Review and Cyber Security Evaluation Tool



7. Training

8. Strategy for Securing Control Systems

Recent Product Releases

Alerts

IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure, 02/25/2016

Advisories

ICSA-16-049-01 B+B SmartWorx VESP211 Authentication Bypass Vulnerability, 02/18/2016

ICSA-16-049-02 AMX Multiple Products Credential Management Vulnerabilities, 02/18/2016

ICSA-16-040-01 Tollgrade SmartGrid Sensor Management System Software Vulnerabilities, 02/09/2016

ICSA-16-040-02 Siemens SIMATIC S7-1500 CPU Vulnerabilities, 02/09/2016

ICSA-16-033-01 Sauter moduWeb Vision Vulnerabilities, 02/02/2016

ICSA-16-033-02 GE SNMP/Web Interface Vulnerabilities, 02/02/2016

ICSA-16-028-01 Westermo Industrial Switch Hard-coded Certificate Vulnerability, 01/28/2016

ICSA-16-026-01 MICROSYS PROMOTIC Memory Corruption Vulnerability, 01/26/2016

ICSA-16-026-02 Rockwell Automation MicroLogix 1100 PLC Overflow Vulnerability, 01/26/2016

ICSA-16-021-01 CAREL PlantVisor Enhanced Authentication Bypass Vulnerability, 01/21/2016

ICSA-15-337-02 Hospira Multiple Products Buffer Overflow Vulnerability, 01/21/2016

ICSA-16-019-01 Siemens OZW672 and OZW772 XSS Vulnerability, 01/19/2016

ICSA-16-014-01 Advantech WebAccess Vulnerabilities, 01/14/2016

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 Published January/February 2016

ICS-CERT appreciates having worked with the following researchers:

- Independent researcher Maxim Rupp, ICSA-16-049-01 B+B SmartWorx VESP211 Authentication Bypass Vulnerability, 02/18/2016.
- Independent researcher Maxim Rupp, ICSA-16-040-01 Tollgrade SmartGrid Sensor Management System Software Vulnerabilities, 02/09/2016.
- Martin Jartelius and John Stock of Outpost24, ICSA-16-033-01 Sauter moduWeb Vision Vulnerabilities, 02/02/2016.
- Independent researcher Karn Ganeshen, ICSA-16-033-02 GE SNMP/Web Interface Vulnerabilities, 02/02/2016.
- Independent researcher Neil Smith, ICSA-16-028-01 Westermo Industrial Switch Hard-coded Certificate Vulnerability, 01/28/2016.
- Security researcher Praveen Darshanam of Versa Networks, ICSA-16-026-01 MICROSYS PROMOTIC Memory Corruption Vulnerability, 01/26/2016.
- David Atch of CyberX, ICSA-16-026-02 Rockwell Automation MicroLogix 1100 PLC Overflow Vulnerability, 01/26/2016.
- Independent researcher Maxim Rupp, ICSA-16-021-01 CAREL PlantVisor Enhanced Authentication Bypass Vulnerability, 01/21/2016.
- Jeremy Richards of SAINT Corporation, ICSA-15-337-02 Hospira Multiple Products Buffer Overflow Vulnerability, 01/21/2016.
- Independent researcher Aditya Sood, ICSA-16-019-01 Siemens OZW672 and OZW772 XSS Vulnerability, 01/19/2016.
- Ilya Karpov of Positive Technologies, Ivan Sanchez, Andrea Micalizzi, Ariele Caltabiano, Fritz Sands, Steven Seeley, and an anonymous researcher, ICSA-16-014-01 Advantech WebAccess Vulnerabilities, 01/14/2016.

Follow ICS-CERT on Twitter: @icscert

Upcoming Events

April 2016

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

April 4–8

Idaho Falls, Idaho

Course Closed

May 2016

ICSJWG 2016 Spring Meeting

May 3-5

Scottsdale, Arizona

Course description and registration

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

May 9-13

Idaho Falls, Idaho

Course description and registration

For a current schedule of events that the ICS-CERT is supporting and may be of interest to control system individuals involved in security, go to https://ics-cert.us-cert.gov/Calendar.

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.

Reporting Incidents

Please let us know if you have experienced a cyber intrusion or anomalous activity on your network. Reporting to ICS-CERT is completely voluntary; however, your information is extremely useful for understanding the current threat landscape, including the techniques adversaries are using, types of malware, possible intent of campaigns, and sectors targeted. Prompt and detailed reporting can lead to early detection and prevent incidents from occurring against the Nation's critical infrastructure.

Your information will be protected. ICS-CERT's policy is to keep confidential any reported information specific to your organization or activity. Organizations can also leverage the PCII program to further protect and safeguard their information (http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program).

What is the publication schedule for this newsletter?

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://ics-cert.us-cert.gov.

Please direct all questions or comments about the content or suggestions for future content to ICS CERT at: ics-cert@hq.dhs.gov.

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://www.us-cert.gov/forms/feedback.