NCCIC

ICS-CERT MONITOR

Contents

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 at the following URL: 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: https://ics-cert.us-cert.gov/

Report an ICS incident to ICS-CERT

Report an ICS software vulnerability

Get information about reporting

GovDelivery

ICS-CERT launched a new digital subscription system with GovDelivery 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 at the following URL: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

Downloading PGP/GPG Keys

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

ICS-CERT Services

ICS-CERT Training

In this issue of the Monitor, we highlight ICS-CERT Training. In March, ICS-CERT completed its 100th Cybersecurity 301, or Red Team/Blue Team, training course (see article on Page 4).

NCCIC/ICS-CERT training courses and workshops share in-depth defense strategies and up-to-date information on cyber threats and mitigations for vulnerabilities with the goal of improving cybersecurity preparedness in the control systems community. Training is a fundamental component of any robust cybersecurity strategy. ICS-CERT supports critical infrastructure (CI) sectors and the control system community by offering multiple training courses, ranging in difficulty at numerous locations around the country and online. ICS-CERT provides these trainings specifically for the personnel responsible for the oversight, design, and operation of control systems. All training options are offered free of charge with no cost to the student, and a certificate of completion is available after each course. In FY 2016, the Training team updated the online and classroom course materials multiple times to include the latest data on threats and vulnerabilities and their appropriate mitigations from cybersecurity experts. ICS-CERT is currently sponsoring 15 training courses and developing two more.

For more about ICS-CERT training, go to https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT. For a list of upcoming training events, go to https://ics-cert.us-cert.gov/Calendar.

Cyber Security Evaluation Tool

The Cyber Security Evaluation Tool (CSET™) is a self-contained software tool that runs on a desktop or laptop computer. The tool provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture, and does not require connection to the Internet or to any control system or corporate network. CSET™ also does not transmit information to The Department of Homeland Security (DHS) or any government or commercial entity and does not report information to anyone except the person using the tool. CSET™ guides asset owners and operators through a step-by-step process to evaluate industrial control system (ICS) and information technology (IT) network security practices.

NCCIC/ICS-CERT released CSET™ version 8.0 in September 2016. DHS developed the CSET™ application and now offers it at no cost to end users. Although we have temporarily suspended development of the tool during the Continuing Resolution, NCCIC/ICS-CERT is committed to developing and improving the CSET™ in future versions and welcomes user feedback for continuous improvement.

CSET™ is available on the NCCIC/ICS-CERT web site (https://ics-cert.us-cert.gov/) by selecting "Assessments" from the menu on the left.

ICS-CERT Remote Assessments

As a core part of ICS-CERT's mission to reduce risk to the Nation's CI, ICS-CERT provides ICS Private Sector CI Assessments in partnership with CI owner/operators to strengthen their ICS cybersecurity posture. ICS-CERT bases these voluntary assessments on standards, guidelines, and best practices and performs them at the request of the asset owner/operator. The information gained from these assessments provides owner/operators with the understanding necessary to build effective defense-in-depth strategies for enhancing their cybersecurity posture.

ICS Private Sector CI Assessments have gone through quite a few continuous improvement efforts over the past few months. We have moved away from individual assessment offerings (CSET™/DAR/NAVV) and toward a comprehensive assessment process that includes adjusting the assessment based on the needs and situation of that particular asset owner. We also no longer offer stand-alone facilitated CSET™ assessments; however, a CSET™ question set is now included as part of our overall assessment process. Additional information can be found in the ICS Private Sector Critical Infrastructure Assessments Fact Sheet.

ICS Private Sector CI Assessments have also introduced a remote assessment capability in order to keep up with the high demand, while continuing to provide value to more CI asset owners. We recognize that asset owners can have a difficult time making the right people available for multiple day-long meetings and that travel for both asset owners and ICS-CERT assessors can incur significant costs that are not always necessary. ICS-CERT is piloting a new approach to remote assessments that consists of focused sessions typically taking place over multiple weeks. During each session, the team discusses specific topics and reviews assessment results.

This new approach allows greater scheduling flexibility for both asset owners and ICS-CERT assessors, allowing both groups to ensure that they have the appropriate subject matter experts involved for each topic. We are very pleased to share that we have received favorable feedback on this pilot approach and look forward to providing an update on how the remote assessments evolve over the course of the next few months.

Tips for using The Homeland Security Information Network

HSIN
HOMELAND SECURITY INFORMATION NETWORK
The Trusted DHS Information Sharing Environment

Selecting or Creating Custom Library Views

HSIN provides a simple method within any document library to set a custom view. Custom views simplify the process of locating a specific document within the library. This discussion uses the "ICS-CERT Advisories & Reports" document library as an example.

After initially navigating to the "ICS-CERT Advisories & Reports" library, the library path in the gray bar at the top of the display indicates the "All Documents" view, which is the default view for this library.

Click on the "All Documents" link to see a drop-down menu of available views for this library. ICS-CERT created common views to display Alerts, Advisories, Indicator Bulletins, Joint Products, Recent Documents, STIX-TAXII, or other documents. Those views are available to all ICS-CERT users when viewing the "ICS-CERT Advisories & Reports Library." Select one of those views to see how it changes the library display.

At the bottom of the drop-down menu is the "Create View" option, which allows a user to create personal custom views that are available only to that user.

Click on the "Create View" option; on the next screen, choose "Standard View" or select one of the common views as a starting point for the new view. In the "Create View" dialog, enter a name for the view; choose which columns to display and assign their "left-to-right" position in the view. If desired, set up "sort" and "filter" options to further refine the data layout.

Several additional parameter settings are available; we recommend leaving most of them in the default state; at most, change only one at a time until you achieve the desired personal view.

When finished setting view parameters, click the "OK" button (at the top or bottom of the screen) to set the personal view and see the resulting display. If further adjustments are needed, select "Modify this View" from the drop-down menu to return to the View dialog.

100th Red Team/Blue Team Training

In March, ICS-CERT Training completed the 100th session of its Industrial Control Systems Cybersecurity (301) training course, also called Red Team/Blue Team training. ICS-CERT began offering the course in 2007 and has now, after the 100th session, trained over 4,000 cybersecurity professionals.

The purpose of the course is to train, free of charge, cybersecurity professionals in the defense of the industrial control system networks in use throughout the Nation's 16 CI sectors. Since 2007, this course has trained cybersecurity professionals from each CI sector, all 50 U.S. states, and multiple other countries. ICS-CERT's 101, 201, and 202 classes are "regional" training courses that have trained over 12,000 individuals at various locations, but the 301 course is held in Idaho Falls, Idaho, at the Idaho National Laboratory's (INL) CSAC facility, which contains an actual control system environment specifically configured for this course.

The first three days of the five-day course provide hands-on training in how to discover who or what is on a control system network, to identify vulnerabilities, to learn how attackers may exploit vulnerabilities, and to learn defensive and mitigation strategies. The fourth day of training consists of the eight-hour Red Team/Blue Team exercise. Participants on the Red Team attempt to attack a control system network, while participants on the Blue team must defend the network while also maintaining the operations of a batch mixing plant and an electrical distribution supervisory control and data acquisition (SCADA) system. The fifth day consists of a lessons learned exercise and round table discussion.

ICS-CERT is proud of the success of its Training team and its reaching this impressive milestone. For more information about ICS-CERT training or to sign up for the Red Team/Blue Team training, or any of ICS-CERT's other cyber security training, go to https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

ICSJWG Meetings

ICSJWG Spring 2017 Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) 2017 Spring Meeting was held at Loews Hotel in Minneapolis, Minnesota, on April 11–13. This was the largest ICSJWG Meeting to date, bringing together over 325 stakeholders from the ICS community. Over the course of three days, attendees had the opportunity to network and interact through demonstrations, presentations, lightning rounds, and panels.

Highlights of the 2017 Spring Meeting:

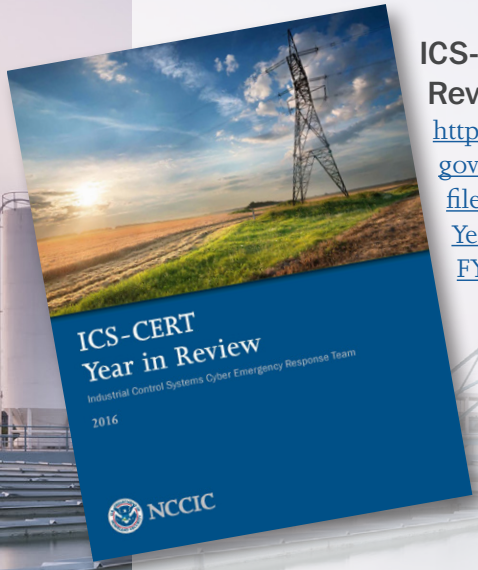
- Keynote presentations from:
  - Ben Miller, Dragos—Director, Threat Operations
  - Marty Edwards, Director of ICS-CERT.
- ICSJWG's Third Vendor Expo.
- "Ask Me Anything" session with Marty Edwards.

ICSJWG Fall 2017 Meeting Preview

ICS-CERT and the ICSJWG are working to finalize the venue for the ICSJWG 2017 Fall Meeting September 12–14, 2017, in Pittsburgh, Pennsylvania! Please save the date and watch for meeting updates.

New ICS-CERT Products Released in March/April 2017

In March and April, ICS-CERT released the 2016 ICS-CERT Year in Review, a Destructive Malware white paper, and two new Assessment fact sheets.

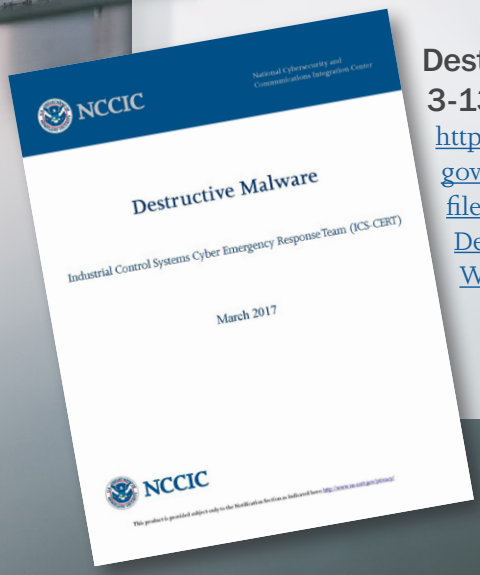


ICS-CERT Year in Review 2016, 3-22-17

https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf

ICS Private Sector Critical Infrastructure Assessments, 3-14-17

https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Private_Sector_Assessments_S508C.pdf



Destructive Malware, 3-13-17

https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf

ICS Federal Critical Infrastructure Assessments, 3-14-17

https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Federal_Assessments_S508C.pdf

Assessments Q&A

How will ICS-CERT use our data?

ICS-CERT publishes an Annual Assessment Report each Fiscal Year, which provides an overview and analysis of assessments conducted by ICS-CERT. The Assessments team completely anonymizes the data used in these reports. Go to https://ics-cert.us-cert.gov/Assessments for examples of this report.

How long does ICS-CERT keep our data?

Protected critical infrastructure information (PCII) is retained and protected permanently or until it is removed at the request of the asset owner.

How much does an assessment cost?

Because ICS-CERT's assessment services are based on Congressional funding, they are available as onsite or remote facilitated assessments for CI asset owners and operators at no cost.

How do I schedule an assessment?

To schedule an assessment, email the ICS-CERT assessment team at ics-assessments@hq.dhs.gov. First, we will set up an "Offerings Call." During this call, we will discuss the assessments we have to offer and determine if any of them are a good fit for your organization.

What do I need to submit prior to scheduling an assessment?

After the "Offerings Call," should you choose to proceed with an assessment, we will send you the pre-assessment documents (Request for Technical Assistance, Logistics Form Request, and PCII Express Statement). After you have submitted these documents and DHS Legal has approved them, we will request network diagrams and inventory lists to review and discuss prior to scheduling.

How do I transmit my data to DHS?

Data is transmitted through HSIN (https://www.dhs.gov/homeland-security-information-network-hsin) or through secure Sharefile (for larger files).

For more information, see ICS-CERT's Assessment FAQs and Fact Sheets.

PCII Q&A

What are the requirements for accessing PCII?

PCII is made available only to those Federal, state, and local government employees and their contractors who

- are trained in the proper handling and safeguarding of PCII;
- have homeland security responsibilities as specified in the CII Act, the Final Rule, and policies and procedures issued by the PCII Program;
- have a need to know the specific information; and
- sign a Non-Disclosure Agreement (non-Federal employees).

In addition to the above requirements, government contractors must modify relevant contracts to comply with requirements of the PCII Program. The contract modification is not a prerequisite to accessing PCII; however, the contractor must contractually acknowledge its responsibilities with respect to PCII as soon as practicable. To avoid delay or interruption of access to PCII, the PCII Program Manager or a PCII Officer can certify contractors. The PCII Accreditation Program is one part of a structure designed to ensure consistent application of uniform program standards and requirements by all participating entities.

For additional questions and answers, see the PCII FAQs.

ICS-CERT Assessment Activity for March/April 2017

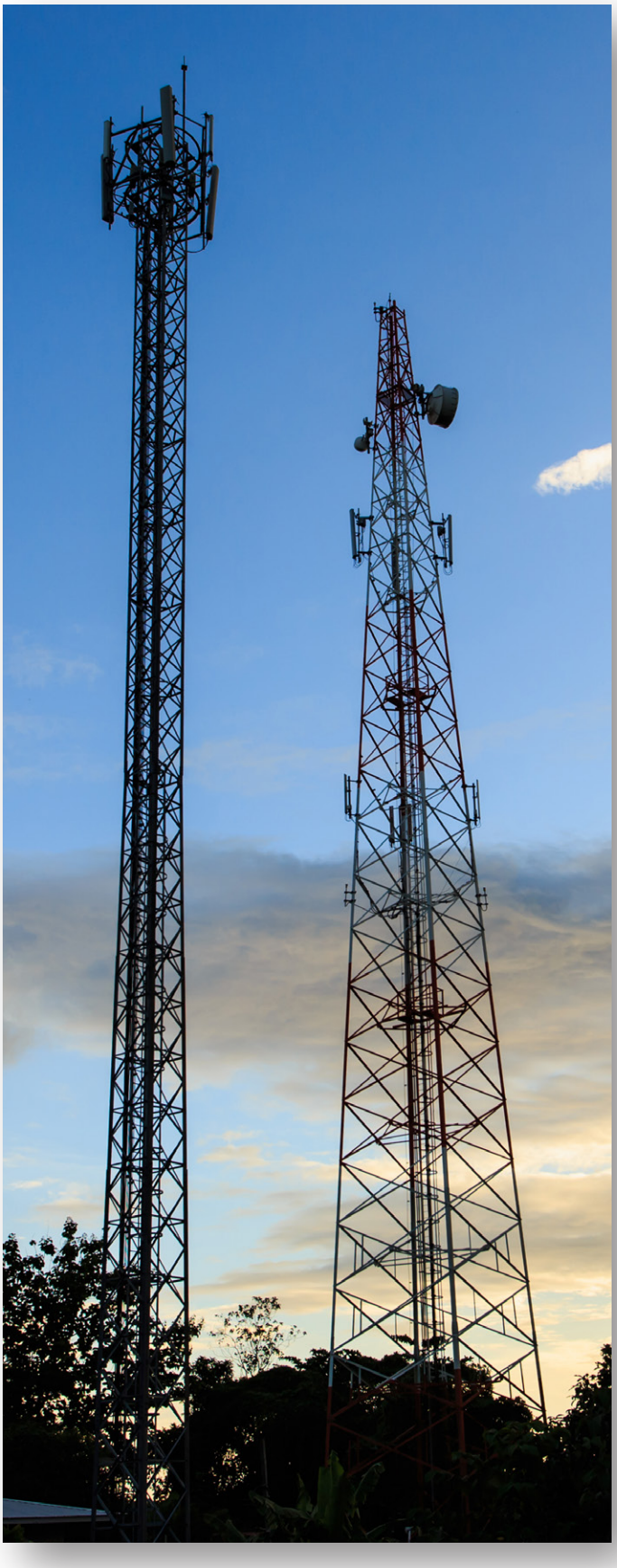
ICS-CERT conducts onsite cybersecurity assessments of ICSs to help strengthen the cybersecurity posture of CI owners and operators and of ICS manufacturers. In March/April 2017, ICS-CERT conducted 15 onsite assessments across two sectors (Table 1). Of these 15 assessments, 10 were Design Architecture Review (DAR) assessments and five were Network Architecture Verification and Validation (NAVV) assessments (Table 2). For detailed information on ICS-CERT™, DAR, and NAVV assessments, go to https://ics-cert.us-cert.gov/assessments.

Table 1: Assessments by sector, March/April 2017.

Assessments by Sector	March 2017	April 2017	March/April Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams	10	4	14
Defense Industrial Base			
Emergency Services			
Energy		1	1
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems			
Monthly Totals	10	5	15 Total Assessments

Table 2. Assessments by type, March/April 2017.

Assessments by Type	March 2017	April 2017	March/April Totals
CSET ™			
DAR	6	4	10
NAVV	4	1	5
Monthly Totals	10	5	15 Total Assessments



Recent Product Releases

Alerts

ICS-ALERT-17-102-01A BrickerBot Permanent Denial-of-Service Attack (Update A), April 18, 2017

ICS-ALERT-17-089-01 Miele Professional PG 8528 Vulnerability, March 30, 2017

ICS-ALERT-17-073-01A MEMS Accelerometer Hardware Design Flaws (Update A), April 11,

Advisories

ICSA-17-117-01 GE Multilin SR Protective Relays, April 27, 2017

ICSA-17-096-01A Certec EDV GmbH atvise scada (Update A), April 27, 2017

ICSA-17-115-01 BLF-Tech LLC VisualView HMI, April 25, 2017

ICSA-17-115-02 Sierra Wireless AirLink Raven XE and XT, April 25, 2017

ICSA-17-115-03 Hyundai Motor America Blue Link, April 25, 2017

ICSA-17-103-01 Wecon Technologies LEVI Studio HMI Editor, April 13, 2017

ICSA-17-103-02 Schneider Electric Modicon M221 PLCs and SoMachine Basic, April 13, 2017

ICSA-17-101-01 Schneider Electric Modicon Modbus Protocol, April 11, 2017

ICSA-17-094-01 Schneider Electric Interactive Graphical SCADA System Software, April 4, 2017

ICSA-17-094-02 Marel Food Processing Systems, April 4, 2017

ICSA-17-094-03 Rockwell Automation Allen-Bradley Stratix and Allen-Bradley ArmorStratix, April 4, 2017

ICSA-17-089-01 Schneider Electric Wonderware InTouch Access Anywhere, March 30, 2017

ICSA-17-089-02 Schneider Electric Modicon PLCs, March 30, 2017

ICSA-17-087-01 Siemens RUGGEDCOM ROX I, March 28, 2017

ICSA-17-087-02 3S-Smart Software Solutions GmbH CODESYS Web Server, March 28, 2017

ICSA-17-082-01 LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA ME LAquis SCADA, March 23, 2017

ICSMA-17-082-01 BD Kiestra PerformA and KLA Journal Service Applications Hard-Coded Passwords Vulnerability, March 23, 2017

ICSA-17-047-01 Rockwell Automation Connected Components Workbench, March 21, 2017

ICSA-17-047-02 Rockwell Automation FactoryTalk Activation, March 21, 2017

ICSA-17-075-01 LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA ME LAquis SCADA, March 16, 2017

ICSA-17-073-01 Fatek Automation PLC Ethernet Module, March 14, 2017

ICSA-17-068-01 Schneider Electric ClearSCADA, March 9, 2017

ICSA-17-066-01 Schneider Electric Wonderware Intelligence, March 7, 2017

ICSA-17-061-01 Eaton xComfort Ethernet Communication Interface, March 2, 2017

ICSA-17-061-02 Schneider Electric Conext ComBox, March 2, 2017

ICSA-17-061-03 Siemens SINUMERIK Integrate and SINUMERIK Operate, March 2, 2017

Follow ICS-CERT on Twitter: @icscert

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 March/April 2017

ICS-CERT appreciates having worked with the following researchers:

- Sebastian Neef of Internetwache.org, ICSA-17-096-01A Certec EDV GmbH atvise scada (Update A), April 27, 2017
- Karn Ganeshen, ICSA-17-115-01 BLF-Tech LLC VisualView HMI, April 25, 2017
- Will Hatzer and Arjun Kumar working with Rapid7, ICSA-17-115-03 Hyundai Motor America Blue Link, April 25, 2017
- Andrea (rgod) Micalizzi, working with iDefense Labs, ICSA-17-103-01 Wecon Technologies LEVI Studio HMI Editor, April 13, 2017
- Simon Heming, Maik Brüggemann, Hendrik Schwartke, and Ralf Spenneberg of Open Source Security, ICSA-17-103-02 Schneider Electric Modicon M221 PLCs and SoMachine Basic, April 13, 2017
- Eran Goldstein of CRITIFENCE, ICSA-17-101-01 Schneider Electric Modicon Modbus Protocol, April 11, 2017
- Karn Ganeshen, ICSA-17-094-01 Schneider Electric Interactive Graphical SCADA System Software, April 4, 2017
- Daniel Lance, ICSA-17-094-02 Marel Food Processing Systems, April 4, 2017
- Ruslan Habalov and Jan Bee of the Google ISA Assessments Team, ICSA-17-089-01 Schneider Electric Wonderware InTouch Access Anywhere, March 30, 2017
- David Formby and Raheem Beyah of Georgia Tech and Fortiphyd Logic, Inc., ICSA-17-089-02 Schneider Electric Modicon PLCs, March 30, 2017
- Maxim Rupp, ICSA-17-087-01 Siemens RUGGEDCOM ROX I, March 28, 2017
- David Atch of CyberX, ICSA-17-087-02 3S-Smart Software Solutions GmbH CODESYS Web Server, March 28, 2017
- Karn Ganeshen, working with Trend Micro's Zero Day Initiative (ZDI), ICSA-17-082-01 LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA ME LAquis SCADA, March 23, 2017
- Ivan Sanchez, ICSA-17-047-01 Rockwell Automation Connected Components Workbench, March 21, 2017
- Karn Ganeshen, ICSA-17-075-01 LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA ME LAquis SCADA, March 16, 2017
- Sergey Temnikov and Vladimir Dashchenko of Kapersky Lab's Critical Infrastructure Defense Team, ICSA-17-068-01 Schneider Electric ClearSCADA, March 9, 2017
- Maxim Rupp, ICSA-17-061-01 Eaton xComfort Ethernet Communication Interface, March 2, 2017
- Arik Kublanov and Mark Liapustin of Nation-E Ltd, ICSA-17-061-02 Schneider Electric Conext ComBox, March 2, 2017

Upcoming Events

June 2017

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

June 5-9

Idaho Falls, Idaho

Closed

June 2017

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

June 19-23

Idaho Falls, Idaho

Closed

NOTE: The Industrial Control Systems Cybersecurity (301) Training is not currently scheduled to be presented in July.

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.

PCII Protection – Your Information Will Be Protected

Industry partners may request protection under the Critical Infrastructure Information Act of 2002 when submitting information to ICS-CERT. If the proper process is followed and ICS-CERT validates that information, it becomes PCII. ICS-CERT's policy is to keep confidential any reported information specific to your organization or activity. PCII protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data. PCII can only be accessed in accordance with strict safeguarding and handling requirements. Only trained and certified federal, state, and local government employees or contractors may access PCII. (http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program).

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.

Report an incident.

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.

ICS-CERT publishes the ICS-CERT Monitor bimonthly, six times a year.

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.