NCCIC

ICS-CERT MONITOR

Contents

ICS-CERT News

Situational Awareness

Onsite Assessment Summary

Recent Product Releases

Coordinated Vulnerability Disclosure

Upcoming Events

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 any questions related to this report, please contact NCCIC Customer Service at:

U.S. Toll Free: (888) 282-0870

Email: ncciccustomerservice@hq.dhs.gov

Report an ICS incident to ICS-CERT

Report an ICS software vulnerability

Get information about reporting

Granicus

ICS-CERT launched a new digital subscription system with Granicus to help you stay informed. By signing up for Granicus, 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 News

Regional Training in Japan

At the invitation of Japan's Ministry of Economy, Trade and Industry (METI) and the Information-Technology Promotion Agency (IPA), the Department of Homeland Security (DHS) and the ICS-CERT training team traveled to Tokyo, Japan, to participate in an industrial control system (ICS) cybersecurity joint training from September 19th to the 26th. This event was held at the Industrial Cyber Security Center of Excellence (ICSCoE), established in April 2017 to help combat Japan's shortfall of cybersecurity manpower.

During the first week, the ICS-CERT team provided training sessions to ICSCoE students. The students attended two days of lecture and discussions, followed by a day of hands-on activities with the equipment ICS-CERT uses for regional training. During the final two days of training, ICS-CERT met with ICSCoE instructors to field questions, share techniques, and assist the ICSCoE instructors in looking at different ways to share information and interact with students. This was the first such training conducted by DHS/ICS-CERT in Japan.

Representatives of METI stated that the training was very beneficial to students not only to enhance their skills and knowledge relative to information provided by ICS-CERT, but also to open their eyes to the advantages of global collaboration in the cybersecurity field.

With a goal of strengthening Japan's cyber defense capabilities against activity directed towards critical infrastructure and the industrial base, METI held

discussions with various companies about the importance of educating leaders in the cybersecurity realm and the concept of building a training program to accomplish that goal. METI and IPA established the ICSCoE with public/private partnerships to develop core human resources for cybersecurity in Japanese critical infrastructure. The ICSCoE has a three-fold mission: Human and Resource Development; Safety and Reliability Assessment of Operations Technology (OT) Systems; and Investigation and Analysis of Cybersecurity Attacks.

Each company carefully selected employees to participate in the ICSCoE curriculum for one year. Upon completion of the training, the students are expected to lead the security strategy and activities of their respective company to improve the security posture of the company and increase the national security of Japan. A valuable result of the ICSCoE training experience is that these young leaders will become senior leaders in future years.

The students are funded for the year by the company they represent and with assistance from the government. There are 76 students in the ICSCoE training. They represent various industries, including utilities, manufacturing, automobile, steel, and chemical.

In addition to the curriculum for the 76 students, ICSCoE conducts a two-day program for executives responsible for cybersecurity, such as CEOs, CIOs, CISOs, directors, and managers. ICSCoE provides the course six times a year. It includes discussions and exercises that are tailored to the industries represented by the attendees.

The ICSCoE plans to serve up to 100 students per year and cover a variety of cyber-related topics including the following: IT/OT basics, such as corporate governance, business continuity, forensics, ICS/supervisory control and data acquisition (SCADA) risks, and cyber exercises; business management and ethics, such as leadership, accounting/finance, presentation skill, budgeting, and relevant legislations; and global case studies.

October is Cybersecurity Awareness Month

October is National Cyber Security Awareness Month, which is an annual campaign to raise awareness about the importance of cybersecurity. The Internet touches almost all aspects of everyone's daily life, whether we realize it or not. National Cyber Security Awareness Month (NCSAM) is designed to engage and educate public and private sector partners through events and initiatives to raise awareness about the importance of cybersecurity, provide them with tools and resources needed to stay safe online, and increase the resiliency of the Nation in the event of a cyber incident.

November is Critical Infrastructure Security and Resilience Month

Critical Infrastructure Security and Resilience Month, observed in the month of November, builds awareness and appreciation of the importance of critical infrastructure and reaffirms the nationwide commitment to keep our critical infrastructure and our communities safe and secure. Securing the nation's infrastructure is a national priority that requires planning and coordination across the entire community.

ICS-CERT Releases Defense-in-Depth Fact Sheet

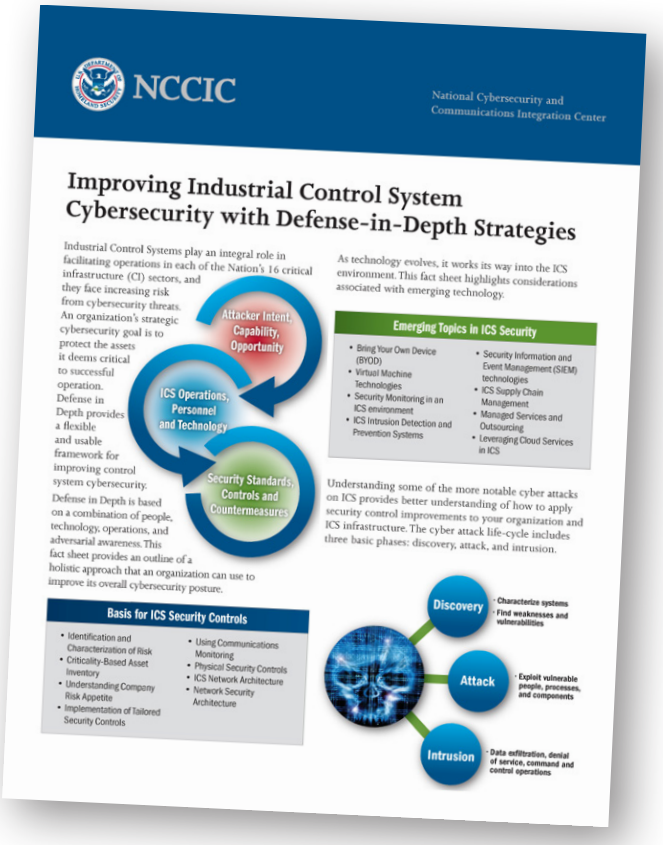
In September, ICS-CERT published a defense-in-depth fact sheet. The fact sheet highlights key points from ICS-CERT's defense-in-depth document, titled "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," published September 13, 2016.

The defense-in-depth recommended practice document provides guidance for developing mitigation strategies for specific cyber threats and direction on how to create a defense-in-depth security program for control system environments. It is a holistic approach, using specific countermeasures implemented in layers to create an aggregated, risk-based security posture. It provides a flexible and useable framework for improving cybersecurity protection and defending against cybersecurity threats and vulnerabilities that could affect ICSs.

ICSs are an integral part of critical infrastructures, helping to facilitate operations in vital industries such as electricity, oil and gas, water, transportation, manufacturing, and chemical manufacturing. The growing issue of cybersecurity and its impact on ICS highlights fundamental risks to the Nation's critical infrastructure. Efficiently addressing ICS cybersecurity issues requires a clear understanding of the current security challenges and specific defensive countermeasures.

The recently released fact sheet provides an introduction to the full document and covers the basis for ICS security controls, emerging topics in ICS security, ICS attack methods, and recommendations for securing ICS.

You can read the defense-in-depth fact sheet here and the full defense-in-depth document here.



NCCIC

National Cybersecurity and Communications Integration Center

Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems play an integral role in facilitating operations in each of the Nation's 16 critical infrastructure (CI) sectors, and they face increasing risk from cybersecurity threats. An organization's strategic cybersecurity goal is to protect the assets it deems critical to successful operation. Defense in Depth provides a flexible and usable framework for improving control system cybersecurity.

Defense in Depth is based on a combination of people, technology, operations, and adversarial awareness. This fact sheet provides an outline of a holistic approach that an organization can use to improve its overall cybersecurity posture.

Attacker Intent, Capability, Opportunity

ICS Operations, Personnel and Technology

Security Standards, Controls and Countermeasures

As technology evolves, it works its way into the ICS environment. This fact sheet highlights considerations associated with emerging technology.

Emerging Topics in ICS Security

- Bring Your Own Device (BYOD)
- Virtual Machine Technologies
- Security Monitoring in an ICS environment
- ICS Intrusion Detection and Prevention Systems
- Security Information and Event Management (SIEM) technologies
- ICS Supply Chain Management
- Managed Services and Outsourcing
- Leveraging Cloud Services in ICS

Understanding some of the more notable cyber attacks on ICS provides better understanding of how to apply security control improvements to your organization and ICS infrastructure. The cyber attack life-cycle includes three basic phases: discovery, attack, and intrusion.

Basis for ICS Security Controls

- Identification and Characterization of Risk
- Criticality-Based Asset Inventory
- Understanding Company Risk Appetite
- Implementation of Tailored Security Controls
- Using Communications Monitoring
- Physical Security Controls
- ICS Network Architecture
- Network Security Architecture

Discovery – Characterize systems; Find weaknesses and vulnerabilities

Attack – Exploit vulnerable people, processes, and components

Intrusion – Data exfiltration, denial of service, command and control operations

Discontinued Wireless Alerts

ICS-CERT discontinued SMS text messages (wireless alerts) in September. To ensure you continue receiving the latest information about security topics and threats, please update your subscriber profile to include an email address. Alternatively, subscribe here using your email address.

Affected ICS-CERT topics:

- Alerts
- Advisories
- Announcements
- Year in Review
- Monitor Newsletter

ICSJWG 2017 Fall Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) hosted the 2017 Fall Meeting in Pittsburgh, Pa., on September 12–14, 2017. The meeting attracted over 300 stakeholders from the ICS community, including ICS asset owners and operators, vendors, academics, and various others. During the three-day event, attendees were able to experience seminars, presentations, and panels on a variety of ICS topics, intimate breakout sessions and lightning-round talks on specific subject matters, engage vendors and workshop demonstrations, and network with one another.

This meeting featured a keynote presentation from Joel Brenner, CIS Senior Research Fellow at MIT, in which he discussed significant sources of cyber insecurity in critical sectors, and highlighted the economic, political, and technological obstacles to creating more secure networks. John Felker, DHS/NCCIC Director of Operations, also provided a keynote address, exploring future services to the ICS community and maintaining ICS expertise in the NCCIC.

Throughout the event, the range of the presentations ensured attendees heard from a variety of perspectives from across the stakeholder community. Presentations were complemented by the availability of vendors and workshops for hands-on engagement. For future meetings, we expect to refine this nexus to ensure that attendees can continue benefitting from the diverse ICS resources that the ICSJWG brings together.

ICSJWG 2018 Spring Meeting Announcement

ICS-CERT is excited to announce the ICSJWG 2018 Spring Meeting, which will take place in Albuquerque, New Mexico, on April 10–12, 2018. Please save the date and we hope that you will join us this spring.

The ICSJWG team will provide more information for the event on the ICSJWG web site when available: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. In the meantime, if you have any questions, feel free to email us at ICSJWG.Communications@hq.dhs.gov.

ICSJWG Webinar Series

The ICS-CERT webinar series continued on October 25, 2017. Michael Schroeder, Director of Programs at 3 Territory Solutions, LLC, presented on "Creating Predictable Fail Safe Conditions for Healthcare Facility-Related Control Systems and Medical Devices by Use of System Segmentation."

If you are interested in participating in future webinars, please contact ICSJWG.Communications@hq.dhs.gov. The ICSJWG team has planned additional webinars for January and March of 2018. If you have a topic you would like to share with the ICSJWG community, please consider an ICSJWG-hosted webinar. For more information, please contact ICSJWG.Communications@hq.dhs.gov.

Updating Antivirus Software in Industrial Control Systems

Antivirus software, when properly deployed and up-to-date, is an important part of a defense-in-depth strategy to guard against malicious software (malware). Such software is widely used in Information Technology (IT) and ICS infrastructures. In business IT environments, it is common practice to configure each antivirus client to update directly from the antivirus vendor; however, because ICS and IT systems require separation by the ICS demilitarized zone (DMZ), ICS systems require different antivirus update methods.

Antivirus Update Strategies for Industrial Control Systems

The recommended secure network architecture for ICS (Figure 1) places the antivirus, Windows Server Update Services (WSUS), and patch server(s) in the control center LAN DMZ. In this architecture, each level should only send or receive traffic to any directly adjacent level, which precludes the antivirus/WSUS/patch server from communicating directly with either the vendor antivirus servers or the organizational antivirus servers.

Although it is more time-consuming to perform regularly, one method to update antivirus software in an ICS system is to download the updates from the vendor antivirus servers to a dedicated host, write the updates to removable media, and use that media to update the AV/WSUS/Patch Server. When using this method, it is important to verify that the update source is legitimate, the hash values of updates are correct, and staff handle the distribution media securely in accordance with the organization's removable media policy.

This method uses the following steps:

- Verify the source of the update.
- Download the update file(s) to a dedicated host (server or workstation).
- Scan the downloaded file(s) for malware.
- Verify the cryptographic hash of each downloaded file(s).
- Scan the removable media for malware or other unexpected data before use to verify its integrity. The safest option is to securely erase the removable media and reformat the drive with the appropriate file system (for flash or magnetic media) or use a new CD or DVD media (for optical media) for each update.
- Write the file(s) to the removable media. Dedicate this media only to updates.
- Lock the media so others cannot write to it.
- Load the media into the test environment and verify that it has no adverse impact to the test system.
- Re-scan the media for malware or other unexpected data to verify nothing transferred to the removable media from the test environment host.
- Install the update on a non-critical endpoint or segment of the system and verify that it has no adverse impact to the production system.
- Install the update on the remaining hosts.
- Monitor the system for any unusual behavior and verify proper operation of the ICS.

This process is more labor intensive than an automatic chaining of updates, but it is not prohibitively time-consuming. This "sneaker net" method is common in air-gapped networks. Automatically "daisy chaining" the updates, which is similar to the process used in many IT environments, is convenient but not recommended.

Testing and Validation

Testing and validation is a critical step in updating antivirus software in ICS environments. Wherever possible, organizations should use test environments that closely approximate the production environment. If there are no issues after testing, deploy the update into operational systems in order of least criticality: first, the Corporate IT network; next, the ICS DMZ; and finally, the ICS network.

The purpose of updating antivirus software is to ensure a higher level of protection. The resulting higher level of protection reduces the downtime and other adverse impacts that are the consequences of a compromise of the ICS. Tailor this method to the environment to support both the operational and security needs of the organization, and always include verification of the updates, maintain separation of levels to support defense in depth, and adequate testing of updates.

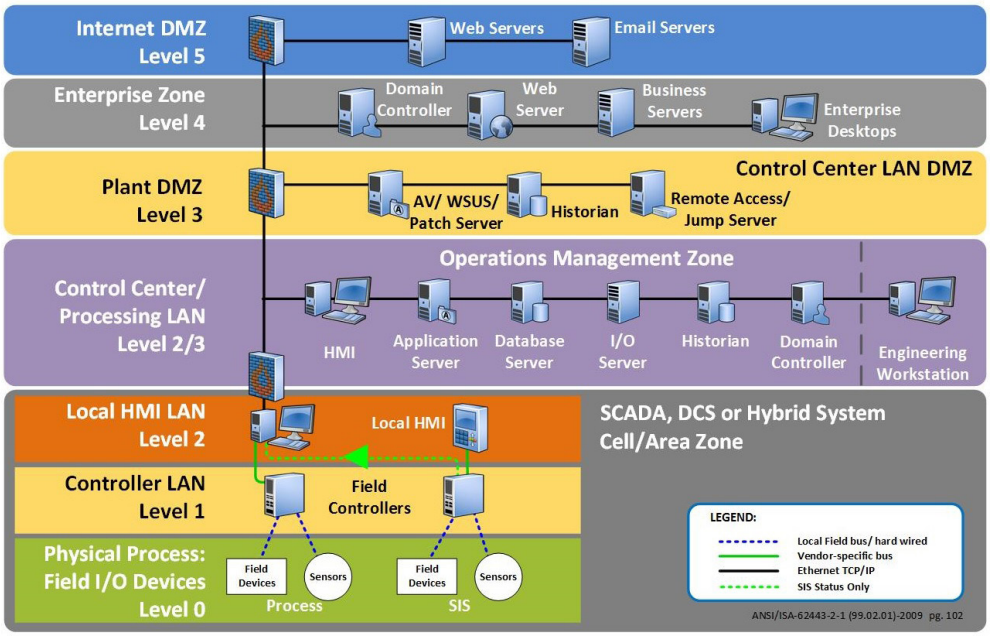


Figure 1. Recommended secure network architecture.

ICS-CERT Assessment Activity for September/October 2017

ICS-CERT conducts onsite cybersecurity assessments of ICSs to help strengthen the cybersecurity posture of critical infrastructure owners and operators and of ICS manufacturers. In September/October 2017, ICS-CERT conducted 30 onsite assessments across three sectors (Table 1). Of these 30 assessments, seven were Cyber Security Evaluation Tool (CSET®) assessments, 11 were Design Architecture Review (DAR) assessments, and 12 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, September/October 2017.

Assessments by Sector	September 2017	October 2017	September/ October Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing	3		3
Dams			
Defense Industrial Base			
Emergency Services			
Energy	11		11
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems	8	8	16
Monthly Totals	22	8	30 Total Assessments

Table 2. Assessments by type, September/October 2017.

Assessments by Type	September 2017	October 2017	September/ October Totals
CSET ™	5	2	7
DAR	8	3	11
NAVV	9	3	12
Monthly Totals	22	8	30 Total Assessments

Recent Product Releases

Advisories

ICSA-17-304-02 Trihedral Engineering Limited VTScada, October 31, 2017

ICSA-17-299-01 Korenix JetNet, October 26, 2017

ICSA-17-292-01 SpiderControl MicroBrowser, October 19, 2017

ICSMA-17-292-01 Boston Scientific ZOOM LATITUDE PRM Vulnerabilities, October 19, 2017

ICSA-17-290-01 Progea Movicon SCADA/HMI, October 17, 2017

ICSA-17-285-01 ProMinent MultiFLEX M10a Controller, October 12, 2017

ICSA-17-285-02 WECON Technology Co., Ltd. LeviStudio HMI Editor, October 12, 2017

ICSA-17-285-03 Envitech Ltd. EnviDAS Ultimate, October 12, 2017

ICSA-17-285-04 NXP Semiconductors MQX RTOS, October 12, 2017

ICSA-17-285-05 Siemens BACnet Field Panels, October 12, 2017

ICSA-17-283-01 LAVA Computer MFG Inc. Ether-Serial Link, October 10, 2017

ICSA-17-283-02 JanTek JTC-200, October 10, 2017

ICSA-17-278-01A GE CIMPLICITY (Update A), October 10, 2017

ICSA-17-271-01A Siemens Ruggedcom ROS, SCALANCE (Update A), October 10, 2017

ICSA-17-278-02 Siemens 7KT PAC1200 Data Manager, October 5, 2017

ICSA-17-264-01 Schneider Electric InduSoft Web Studio, InTouch Machine Edition, September 21, 2017

ICSA-17-264-02 Ctek, Inc. SkyRouter, September 21, 2017

ICSA-17-264-03 Digium Asterisk GUI, September 21, 2017

ICSA-17-264-04 iniNet Solutions GmbH SCADA Webserver, September 21, 2017

ICSA-17-234-05 Saia Burgess Controls PCD Controllers, September 21, 2017

ICSA-17-262-01 PHOENIX CONTACT mGuard Device Manager, September 19, 2017

ICSA-17-257-01 LOYTEC LVIS-3ME, September 14, 2017

ICSA-17-255-01 mySCADA myPRO, September 12, 2017

ICSMA-17-255-01 Philips' IntelliView MX40 Patient Worn Monitor (WLAN) Vulnerabilities, September 12, 2017

ICSA-17-250-01 SpiderControl SCADA Web Server, September 7, 2017

ICSA-17-250-02 PHOENIX CONTACT, Innominate Security Technologies mGuard Firmware, September 7, 2017

ICSMA-17-250-01 i-SENS, Inc. SmartLog Diabetes Management Software, September 7, 2017

ICSMA-17-250-02 Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities, September 7, 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 NCCIC Customer Service at nccicccustomerservice@hq.dhs.gov or toll free at 1-888-282-0870.

Researchers Assisting ICS-CERT with Products Published September/October 2017

ICS-CERT appreciates having worked with the following researchers:

- Karn Ganeshen and Mark Cross, ICSA-17-304-02 Trihedral Engineering Limited VTScada, October 31, 2017
- Mandar Jadhav of the Qualys Vulnerability Signature/Research Team, ICSA-17-299-01 Korenix JetNet, October 26, 2017
- Karn Ganeshen, ICSA-17-292-01 SpiderControl MicroBrowser, October 19, 2017
- Researchers Jonathan Butts and Billy Rios of Whitescope, ICSMA-17-292-01 Boston Scientific ZOOM LATITUDE PRM Vulnerabilities, October 19, 2017
- Karn Ganeshen, ICSA-17-290-01 Progea Movicon SCADA/HMI, October 17, 2017
- Maxim Rupp, ICSA-17-285-01 ProMinent MultiFLEX M10a Controller, October 12, 2017
- Andrea "rgod" Micalizzi, working with iDefense Labs, ICSA-17-285-02 WECON Technology Co., Ltd. LeviStudio HMI Editor, October 12, 2017
- Can Demirel and Deniz Çevik of Biznet Bilisim, ICSA-17-285-03 Envitech Ltd. EnviDAS Ultimate, October 12, 2017
- Scott Gayou, ICSA-17-285-04 NXP Semiconductors MQX RTOS, October 12, 2017
- Maxim Rupp, ICSA-17-283-01 LAVA Computer MFG Inc. Ether-Serial Link, October 10, 2017
- Karn Ganeshan, ICSA-17-283-02 JanTek JTC-200, October 10, 2017
- David Atch of CyberX, ICSA-17-278-01A GE CIMPLICITY (Update A), October 10, 2017
- Maxim Rupp, ICSA-17-278-02 Siemens 7KT PAC1200 Data Manager, October 5, 2017
- Aaron Portnoy, formerly of Exodus Intelligence, ICSA-17-264-01 Schneider Electric InduSoft Web Studio, InTouch Machine Edition, September 21, 2017
- Maxim Rupp, ICSA-17-264-02 Ctek, Inc. SkyRouter, September 21, 2017
- Davy Douhine of RandoriSec, ICSA-17-264-03 Digium Asterisk GUI, September 21, 2017
- Matthias Niedermaier and Florian Fischer, both of Augsburg University of Applied Sciences, ICSA-17-264-04 iniNet Solutions GmbH SCADA Webserver, September 21, 2017
- Davide Fauri of Eindhoven University of Technology, ICSA-17-234-05 Saia Burgess Controls PCD Controllers, September 21, 2017
- Davy Douhine of RandoriSec, ICSA-17-257-01 LOYTEC LVIS-3ME, September 14, 2017
- Karn Ganeshen, ICSA-17-255-01 mySCADA myPRO, September 12, 2017
- Karn Ganeshen, ICSA-17-250-01 SpiderControl SCADA Web Server, September 7, 2017
- Independent researcher Mark Cross, ICSMA-17-250-01 i-SENS, Inc. SmartLog Diabetes Management Software, September 7, 2017
- Independent researcher Scott Gayou, ICSMA-17-250-02 Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities, September 7, 2017

Upcoming Events

February 2018

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

February 5-9

Idaho Falls, Idaho

Course information and registration.

March 2018

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

March 5-9

Idaho Falls, Idaho

Course description; Registration will be available ~90 days prior to the start date.

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: ncciccustomerservice@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 ncciccustomerservice@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.