NCCIC

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 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: http://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 Technical Analysis

Technical analysis includes all aspects of malware analysis; reverse engineering; log and artifact analysis; long-term analysis exploring systemic vulnerabilities, potential future threats, tactics, techniques, and procedures; and other intractable long-term problems. The Advanced Analytical Laboratory (AAL) performs ICS-CERT's primary technical analysis work. The AAL performs most of the malware and artifact analysis. Primary backup support for the AAL and the majority of our applied research projects takes place at Sandia National Laboratory (SNL). The Technical Analysis team also partners with and sponsors research by the Air Force Institute of Technology (AFIT).

The AAL provides research and analysis capabilities in support of ICS-CERT's incident response, assessment, and vulnerability coordination activities. The AAL's expert cybersecurity researchers perform forensic analysis on digital media, reverse engineer malware, and respond to cyber incidents with both onsite and remote capacity. When possible, the AAL performs analytical efforts remotely in a laboratory environment using custom tools and techniques. In some cases, however, onsite analysis is required, and a team deploys to perform analytical efforts directly on the owner's network.

AAL team members receiving an appreciation award from the Department of Homeland Security's (DHS) National Programs and Protection Directorate (NPPD) Under Secretary Suzanne Spaulding.

Be Aware of the Differences in Cybersecurity Architecture Categorizations

Organizations in most critical infrastructure (CI) sectors generally adopt a cybersecurity architecture that offers the most restrictive security to entity equipment requiring the most protection, often referred to as the defensive architecture or Defense in Depth (DiD). Many organizations in CI sectors follow the Purdue Reference Model (Figure 1) for their cybersecurity architectures. The Nuclear Sector follows a model from the Nuclear Regulatory Commission's (NRC) Regulatory Guide 5.71 (Figure 2).

Figure 1 provides a visual representation of the Purdue Reference Model. The figure depicts logical levels that do not necessarily correspond to physical locations inside a plant or manufacturing process.

Level 0 consists of equipment such as sensors, actuators, and other gear at the heart of the physical process, including the data they transmit and receive. Level 1 is the controller level, composed of equipment such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that control processes and send/receive data. Level 1 also includes safety systems, which should always remain stand-alone, connected only to those systems they are responsible for protecting. Level 2 is the machine/process automation echelon of the cybersecurity architecture. This is where the supervisory control part of Supervisory Control and Data Acquisition (SCADA) equipment and information is located. Level 3 is where operations management and historians function, the data acquisition part of SCADA equipment. Level 4 includes plant level systems and communications that include enterprise resource planning (ERP), materials resource planning (MRP), and manufacturing execution systems (MES). Business systems are in Level 5 and contain archives, file servers, and other business equipment and data.

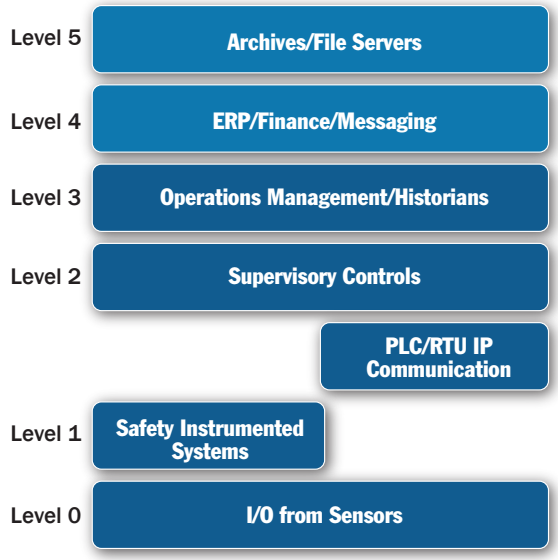


Figure 1. The Purdue Reference Model.

In domestic nuclear power plants, the logical organization of equipment and data/information follows the same basic flow, but the nomenclature is reversed: Level 4 is reserved for systems and data that require the highest degree of cyber security protection, and Level 0 is considered the equivalent of the Internet. Figure 2 illustrates a generalized cyber security defensive architecture (Defense in Depth) from the NRC's Regulatory Guide 5.71. The arrows indicate data flow. The equipment and systems that require the most protection (such as digital equipment associated with safety and important to safety) are located in Level 4.

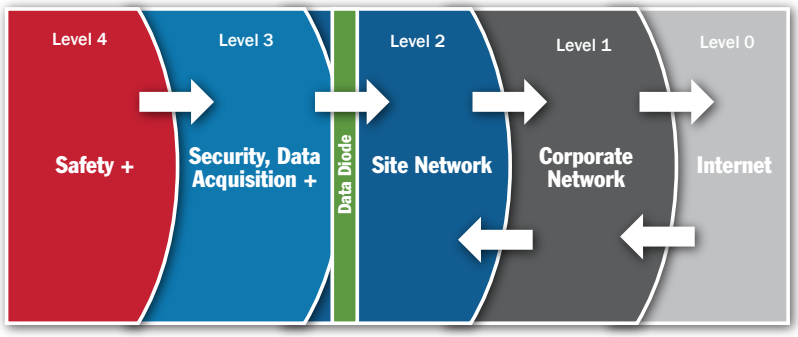


Figure 2. NRC cyber security defensive architecture.

In conversations with domestic nuclear power plant cybersecurity individuals, referring to the Purdue Reference Model would no doubt result in confusion for all involved parties. Understanding the differences in the categorization and labeling of the levels in these two models will help avoid confusion and misunderstanding during important discussions and communications involving cybersecurity.

ICS-CERT FY 2016 Metrics

NCCIC/ICS-CERT FY Metrics	2014	2015	2016
ICS Incident Reports - Tickets	245	295	290
ICS Incident Response Onsite Deployments	4	5	3
ICS Related Vulnerability Reports - Tickets	159	182	187
ICS-CERT Information Products	339	332	274
ICS-CERT Portal Accounts	1,654	1,667	2,360
Distributed or Downloaded CSET®	5,132	7,565	10,249
Onsite Assessments	104	112	130
Professionals Trained	800	1,330	1,622
Number of Training Sessions	21	29	29
ICSJWG Membership	1,726	1,912	2,476
Speaking Engagements	179	343	343

ICSJWG Spring 2017 Meeting

ICS-CERT is excited to announce the Industrial Control Systems Joint Working Group (ICSJWG) 2017 Spring Meeting on April 11-13, 2017, in Minneapolis, Minnesota. Please save the date and watch for the registration links that are coming soon. We look forward to seeing you in Minneapolis! When available, we will post registration information at the following URL: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

NCCIC/ICS-CERT's Advanced Analytical Laboratory Releases Malware Trends White Paper

In November, ICS-CERT released the Advanced Analytical Laboratory's Malware Trends White Paper. As technology advances and new devices join the ranks of those connected to the Internet, new vulnerabilities and challenges in the security of information technology (IT) and operational technology (OT) systems come along for the ride. This white paper explores the changes in malware throughout the past several years, with a focus on what the security industry is most likely to see today; how asset owners can harden existing networks and systems against these attacks; and the expected direction of developments and targets in the coming years.

Assessments Q&A

What is a DAR Assessment?

ICS-CERT's Design Architecture Review (DAR) provides critical infrastructure asset owners and operators with a comprehensive technical review and cyber evaluation of the architecture and components that comprise their industrial control systems (ICS) operations.

This 2-3 day review includes a deep-dive analysis of the operational process—focusing on the underlying ICS network architecture, integration of IT and OT teams, vendor support, monitoring, cybersecurity controls, and all internal and external connections.

The ICS-CERT assessment team works interactively with an asset owner's IT and operations personnel to evaluate the current architecture and processes, with a focus on three key areas:

1. ICS Network Architecture,
2. Asset Inventory, and
3. Protective and Detective Controls.

What is a NAVV Assessment?

ICS-CERT's Network Architecture Verification and Validation (NAVV) is a passive analysis of network header data provided by the asset owner to ICS-CERT from traffic occurring within the ICS network. Using a combination of both open-source and commercially available tools, ICS-CERT presents a strategic visualization of the network header data and device-to-device communications that are occurring within ICS network segments.

ICS-CERT's assessment team works interactively with the asset owner's IT and operations personnel to evaluate the captured network header data, reviewing

- Protocol hierarchy and organization of network traffic,
- Device-to-device communications—including identification of "top-talkers" and the devices generating the most traffic,
- Communications traversing (or attempting to traverse) the ICS network boundary—for verification that the perimeter protections are functioning as intended,
- Potentially misconfigured devices—or those exhibiting suspicious or anomalous behavior, and
- ICS protocol analysis—including an in-depth review of function codes and control parameters within the captured traffic.

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

PCII Q&A

What Protections does the PCII Program Offer?

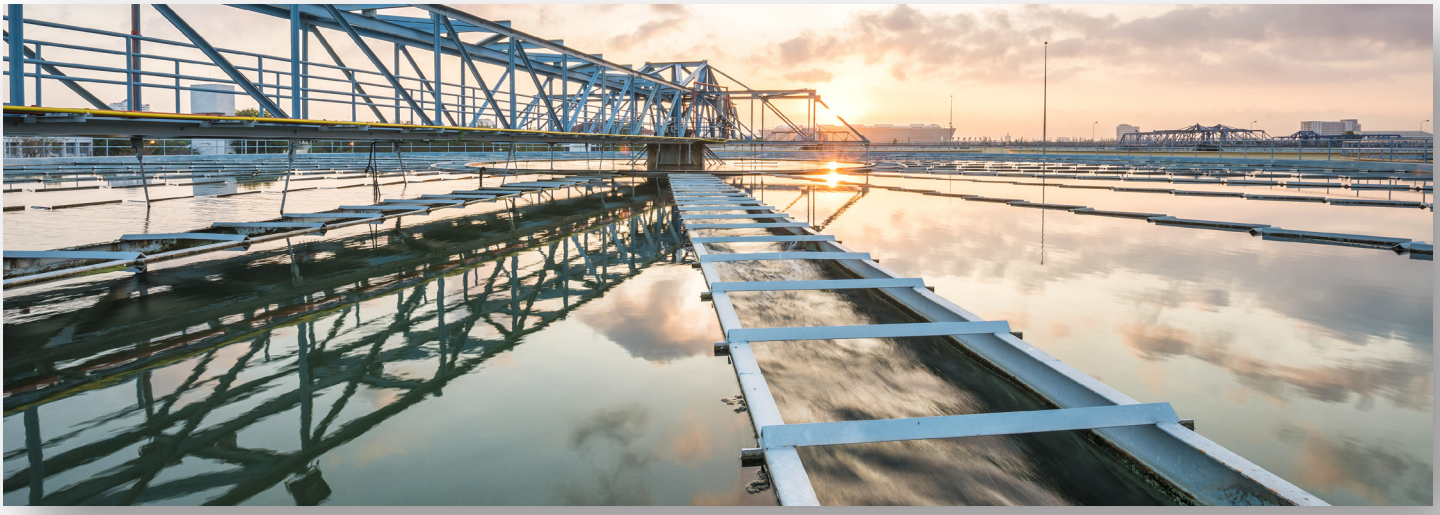
The PCII Program protects all information designated as PCII throughout its lifecycle. PCII Program safeguards ensure that PCII is

- Accessed only by authorized and properly trained individuals,
- Used appropriately for analysis of threats, vulnerabilities, and other homeland security purposes,
- Protected from disclosure under the Freedom of Information Act (FOIA) and similar state and local disclosure laws, and
- Not used directly in civil litigation nor as the basis for regulatory action.

What are the Responsibilities of the PCII Program?

Once the PCII Program validates submitted information as PCII, its mission is to facilitate access to and safeguard PCII. The PCII Program's responsibilities also include establishing guidelines for handling, using, and storing PCII; training users and recipients on safeguarding PCII; and accrediting government entities to handle PCII.

For more information, see the PCII web page and PCII FAQs.



ICS-CERT Assessment Activity for November/December 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 November/December 2016, ICS-CERT conducted 26 onsite assessments across 3 sectors (Table 1). Of these 26 assessments, 5 were Cyber Security Evaluation Tool (CSET®) assessments, 9 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, November/December 2016.

Assessments by Sector	November 2016	December 2016	November/ December Totals
Chemical			
Commercial Facilities		2	2
Communications			
Critical Manufacturing		3	3
Dams			
Defense Industrial Base			
Emergency Services			
Energy	18	3	21
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	18	8	26 Total Assessments

Table 2. Assessments by type, November/December 2016.

Assessments by Type	November 2016	December 2016	November/ December Totals
CSET	3	2	5
DAR	7	2	9
NAVV	8	4	12
Monthly Totals	18	8	26 Total Assessments

Recent Product Releases

Advisories

ICSA-16-357-01 Fidelix FX-20 Series Controllers Path Traversal Vulnerability, December 22, 2016

ICSA-16-357-02 WAGO Ethernet Web-based Management Authentication Bypass Vulnerability, December 22, 2016

ICSA-16-147-01B Environmental Systems Corporation Data Controllers Vulnerabilities (Update B), December 22, 2016

ICSA-16-145-01A Moxa MiiNePort Vulnerabilities (Update A), December 22, 2016

ICSA-16-042-01A Moxa EDR-G903 Secure Router Vulnerabilities (Update A), December 22, 2016

ICSA-16-140-01A Resource Data Management Intuitive 650 TDB Controller Vulnerabilities (Update A), December 22, 2016

ICSA-16-138-01A IRZ RUH2 3G Firmware Overwrite Vulnerability (Update A), December 22, 2016

ICSA-16-355-01 Siemens Desigo PX Web Module Insufficient Entropy Vulnerability, December 20, 2016

ICSA-16-350-01 Fatek Automation PLC WinProladder Stack-Based Buffer Overflow Vulnerability, December 15, 2016

ICSA-16-350-02 OmniMetrix OmniView Vulnerabilities, December 15, 2016

ICSA-16-348-01 Visonic PowerLink2 Vulnerabilities, December 13, 2016

ICSA-16-348-02 Moxa DACenter Vulnerabilities, December 13, 2016

ICSA-16-348-03 Delta Electronics WPLSoft, ISPSoft, and PMSoft Vulnerabilities, December 13, 2016

ICSA-16-348-04 Siemens SIMATIC WinCC and SIMATIC PCS 7 ActiveX Vulnerability, December 13, 2016

ICSA-16-348-05 Siemens S7-300/400 PLC Vulnerabilities, December 13, 2016

ICSA-16-343-01 Moxa MiiNePort Session Hijack Vulnerabilities, December 8, 2016

ICSA-16-343-02 Sauter NovaWeb Web HMI Authentication Bypass Vulnerability, December 8, 2016

ICSA-16-343-03 Adcon Telemetry A850 Telemetry Gateway Base Station Vulnerabilities, December 8, 2016

ICSA-16-343-04 INTERSCHALT VDR G4e Path Traversal Vulnerability, December 8, 2016

ICSA-16-341-01 Tesla Gateway ECU Vulnerability, December 6, 2016

ICSA-16-231-01 Locus Energy LGate Command Injection Vulnerability, December 6, 2016

ICSA-16-336-01 Siemens SICAM PAS Vulnerabilities, December 1, 2016

ICSA-16-336-02 Moxa NPort Device Vulnerabilities, December 1, 2016

ICSA-16-336-03 Mitsubishi Electric MELSEC-Q Series Ethernet Interface Module Vulnerabilities, December 1, 2016

ICSA-16-336-04 Advantech SUSIAccess Server Vulnerabilities, December 1, 2016

ICSMA-16-306-01 Smiths-Medical CADD-Solis Medication Safety Software Vulnerabilities, December 1, 2016

ICSA-16-334-01 Emerson Liebert SiteScan XML External Entity Vulnerability, November 29, 2016

ICSA-16-334-02 Emerson DeltaV Easy Security Management Application Vulnerability, November 29, 2016

ICSA-16-334-03 Emerson DeltaV Wireless I/O Card Open SSH Port Vulnerability, November 29, 2016

ICSA-16-327-01 Siemens SIMATIC CP 1543-1 Vulnerabilities, November 22, 2016

ICSA-16-327-02 Siemens SIMATIC CP 343-1/CP 443-1 Modules and SIMATIC S7-300/S7-400 CPUs Vulnerabilities, November 22, 2016

ICSA-16-322-01 Vanderbilt Industries Siemens IP CCTV Cameras Vulnerability, November 17, 2016

ICSA-16-322-02 Moxa SoftCMS Vulnerabilities, November 17, 2016

ICSA-16-320-01 Lynxspring JENEsys BAS Bridge Vulnerabilities, November 15, 2016

ICSA-16-315-01A CA Unified Infrastructure Management Directory Traversal Vulnerability (Update A), November 15, 2016

ICSA-16-313-01 Phoenix Contact ILC PLC Authentication Vulnerabilities, November 8, 2016

ICSA-16-313-02A Siemens Industrial Products Local Privilege Escalation Vulnerability (Update A), November 22, 2016

ICSA-16-313-03 OSIsoft PI System Incomplete Model of Endpoint Features Vulnerability, November 8, 2016

ICSA-16-308-01 Moxa OnCell Security Vulnerabilities, November 3, 2016

ICSA-16-308-02A Schneider Electric Magelis HMI Resource Consumption Vulnerabilities (Update A), November 22, 2016

ICSA-16-308-03 Schneider Electric IONXXXX Series Power Meter Vulnerabilities, November 3, 2016

ICSA-16-306-01 Schneider Electric ConneXium Buffer Overflow Vulnerability, November 1, 2016

ICSA-16-306-02 IBHsoftec S7-SoftPLC CPX43 Heap-based Buffer Overflow Vulnerability, November 1, 2016

ICSA-16-306-03 Schneider Electric Unity PRO Control Flow Management Vulnerability, November 1, 2016

Other Reports

NCCIC/ICS-CERT Advanced Analytical Laboratory Malware Trends White Paper, November 1, 2016

Follow ICS-CERT on Twitter: @icscert

Open Source Situational Awareness Highlights

91% Of Cyberattacks Start With A Phishing Email

2016-12-13

http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

FACT SHEET: Release of the Joint United States-Canada Electric Grid Security and Resilience Strategy

2016-12-12

https://www.whitehouse.gov/the-press-office/2016/12/12/fact-sheet-release-joint-united-states-canada-electric-grid-security-and

DHS helps you make your control systems more secure

2016-11-28

http://www.csoonline.com/article/3143729/security/dhs-helps-you-make-your-control-systems-more-secure.html

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 November/December 2016

ICS-CERT appreciates having worked with the following researchers:

- Researcher Semen Rozhkov of Kaspersky, ICSA-16-357-01 Fidelix FX-20 Series Controllers Path Traversal Vulnerability, December 22, 2016
- Independent researcher Maxim Rupp, ICSA-16-357-02 WAGO Ethernet Web-based Management Authentication Bypass Vulnerability, December 22, 2016
- Independent researcher Maxim Rupp, ICSA-16-147-01B Environmental Systems Corporation Data Controllers Vulnerabilities (Update B), December 22, 2016
- Independent researcher Karn Ganeshen, ICSA-16-145-01A Moxa MiiNePort Vulnerabilities (Update A), December 22, 2016
- Independent researcher Maxim Rupp, ICSA-16-042-01A Moxa EDR-G903 Secure Router Vulnerabilities (Update A), December 22, 2016
- Independent researcher Maxim Rupp, ICSA-16-140-01A Resource Data Management Intuitive 650 TDB Controller Vulnerabilities (Update A), December 22, 2016
- A researcher working with Trend Micro's Zero Day Initiative (ZDI), ICSA-16-350-01 Fatek Automation PLC WinProladder Stack-Based Buffer Overflow Vulnerability, December 15, 2016
- Bill Voltmer of Elation Technologies LLC, ICSA-16-350-02 OmniMetrix OmniView Vulnerabilities, December 15, 2016
- Independent researcher Aditya K. Sood, ICSA-16-348-01 Visonic PowerLink2 Vulnerabilities, December 13, 2016
- Independent researcher Zhou Yu, ICSA-16-348-02 Moxa DACenter Vulnerabilities, December 13, 2016
- Researchers axt and Ariele Caltabiano each working with Trend Micro's ZDI, ICSA-16-348-03 Delta Electronics WPLSoft, ISPSoft, and PMSoft Vulnerabilities, December 13, 2016
- Mingzheng Li from Acorn Network Security Lab, ICSA-16-348-04 Siemens SIMATIC WinCC and SIMATIC PCS 7 ActiveX Vulnerability, December 13, 2016
- Zhu WenZhe from Beijing Acorn Network Technology, ICSA-16-348-05 Siemens S7-300/400 PLC Vulnerabilities, December 13, 2016
- Independent researcher Aditya K. Sood, ICSA-16-343-01 Moxa MiiNePort Session Hijack Vulnerabilities, December 8, 2016
- Independent researcher Maxim Rupp, ICSA-16-343-02 Sauter NovaWeb Web HMI Authentication Bypass Vulnerability, December 8, 2016
- Independent researcher Aditya K. Sood, ICSA-16-343-03 Adcon Telemetry A850 Telemetry Gateway Base Station Vulnerabilities, December 8, 2016
- Independent researcher Maxim Rupp, ICSA-16-343-04 INTER-SCHALT VDR G4e Path Traversal Vulnerability, December 8, 2016
- Tencent's Keen Security Lab, ICSA-16-341-01 Tesla Gateway ECU Vulnerability, December 6, 2016
- Independent researcher Daniel Reich, ICSA-16-231-01 Locus Energy LGate Command Injection Vulnerability, December 6, 2016
- Security researchers Reid Wightman of RevICS Security, Mikael Vingaard, and Maxim Rupp, ICSA-16-336-02 Moxa NPort Device Vulnerabilities, December 1, 2016
- Security researcher Vladimir Dashchenko of Critical Infrastructure Defense Team, Kaspersky Lab, ICSA-16-336-03 Mitsubishi Electric MELSEC-Q Series Ethernet Interface Module Vulnerabilities, December 1, 2016
- Researcher rgod working with ZDI, ICSA-16-336-04 Advantech SUSIAccess Server Vulnerabilities, December 1, 2016
- Researcher Evgeny Ermakov from Kaspersky Lab, ICSA-16-334-01 Emerson Liebert SiteScan XML External Entity Vulnerability, November 29, 2016
- Zhou Yu working with Trend Micro's ZDI and Gu Ziqiang from Huawei Weiran Labs, ICSA-16-322-02 Moxa SoftCMS Vulnerabilities, November 17, 2016
- Independent researcher Maxim Rupp, ICSA-16-320-01 Lynxspring JENEsys BAS Bridge Vulnerabilities, November 15, 2016
- Independent researcher Andrea Micalizzi, working with ZDI, ICSA-16-315-01A CA Unified Infrastructure Management Directory Traversal Vulnerability (Update A), November 8, 2016
- Matthias Niedermaier and Michael Kapfer of HSASec Hochschule Augsburg, ICSA-16-313-01 Phoenix Contact ILC PLC Authentication Vulnerabilities, November 8, 2016
- Independent researcher Maxim Rupp, ICSA-16-308-01 Moxa OnCell Security Vulnerabilities, November 3, 2016
- Independent researcher Karn Ganeshen, ICSA-16-308-03 Schneider Electric IONXXXX Series Power Meter Vulnerabilities, November 3, 2016
- Security researcher George Lashenko of CyberX, ICSA-16-306-01 Schneider Electric ConneXium Buffer Overflow Vulnerability, November 1, 2016
- Ariele Caltabiano (kimiya) working with Trend Micro's ZDI, ICSA-16-306-02 IBHsoftec S7-SoftPLC CPX43 Heap-based Buffer Overflow Vulnerability, November 1, 2016
- Avihay Kain and Mille Gandelsman of Indegy, ICSA-16-306-03 Schneider Electric Unity PRO Control Flow Management Vulnerability, November 1, 2016

Upcoming Events

February 2017

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

February 6–10

Idaho Falls, Idaho

Closed

March 2017

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

March 13–17

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.

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. Protected Critical Infrastructure Information (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.

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.

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.