



**Homeland  
Security**

# ICS-CERT MONITOR



## Contents

ICS-CERT Services

ICS-CERT News

Onsite Assessment Summary

Recent Product Releases

Open Source Situational  
Awareness Highlights

Coordinated Vulnerability Disclosure

Upcoming Events

## 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](mailto: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 here:

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

This product is provided "as is" for informational purposes only. DHS does not provide any warranties of any kind regarding any information contained herein. DHS does not endorse any commercial product or service referenced in this publication or otherwise.

## ICS-CERT Services

### ICS-CERT Incident Response

*In this issue of the Monitor, we highlight ICS-CERT Incident Response*

The incident response team responds to and helps mitigate cybersecurity incidents impacting industrial control systems (ICSs) in each of the 16 critical infrastructure (CI) sectors across the United States. At the request of CI asset owners after a cyber incident, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides incident response services to assess the extent of the compromise, identify the threat actor's techniques and tactics, and assist the asset owner to develop strategies for mitigation, recovery, and improving cyber defenses for the future. ICS-CERT also provides onsite incident response support, conducts technical analysis of artifacts and malware, develops mitigation strategies for owners and operators, and provides configuration analysis on new systems to ensure sufficient detection and prevention of the evolving threats.

ICS-CERT collaborates with international and private sector Computer Emergency Readiness Teams (CERTs) to share control systems-related security incidents and mitigation measures. The coordination among these partners provides ICS-CERT with a unique perspective of the overall cyber risk landscape and emerging threats. ICS-CERT conveys this information through outreach activities, briefings, and information products, such as alerts and advisories, as well as technical information papers that recommend strategies for improving cyber defense.



Sharing information about cyber incidents is essential to improving the overall security posture of our Nation's CI. ICS-CERT is able to leverage the breadth of knowledge available through our government and community partnerships to improve awareness and provide actionable information to the entire community, without disclosing the identity or sensitive information about the reporting organization. ICS-CERT encourages CI asset owners to contact ICS-CERT for assistance with responding to a cyber incident affecting the control systems environment. Under the PCII Program, your information will be protected from public disclosure under the Freedom of Information Act (FOIA) and similar state and local disclosure laws and from use in civil litigation.

Go to <https://ics-cert.us-cert.gov/> for more information and to <https://ics-cert.us-cert.gov/Report-Incident> to report an incident.

## Presidential Policy Directive on Cyber Incident Coordination

On July 26th, President Obama issued a Presidential Policy Directive (PPD) concerning cyber incident coordination among federal agencies. This directive, PPD-41 and an accompanying annex, identify the “principles governing the Federal Government’s response to any cyber incident, whether involving government or private sector entities.” PPD-41 further delineates between cyber incidents and significant cyber incidents, with a significant incident being “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.”

The PPD lays out five principles for incident response through three concurrent lines of effort. The five principles include 1) shared responsibility, 2) risk-based response, 3) respecting affected entities, 4) unity of governmental effort, and 5) enabling restoration and recovery. The three lines of effort are 1) threat response, 2) asset response, 3) and intelligence support and related activities. When a federal agency is the affected entity, it will follow a fourth line of effort “to manage the effects of the cyber incident on its operations, customers, and workforce.”

The National Cybersecurity and Communications Integration Center (NCCIC), acting under the Department of Homeland Security (DHS), will lead a Cyber Unified Coordination Group (UCG) in federal “asset response” activities. The Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTS), acting under the Department of Justice (DOJ) will lead “threat response” activities. DHS’s U.S. Secret Service (USSS) and U.S. Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI) also play a crucial



role in threat response. The Cyber Threat Intelligence Integration Center (CTIIC), acting under the Office of the Director of National Intelligence (ODNI) will lead “intelligence support and related activities.”

Asset response focuses on the assets of the victim or potential targets of malicious activity, while threat response includes identifying, pursuing, and disrupting malicious cyber actors and activity. To illustrate the difference between asset response and threat response, think of a cyber incident as a fire in the physical world. The NCCIC, which will lead and provide asset response, would be the equivalent of a firefighter. They put out the fire and help the owner rebuild with fire prevention in mind. Federal law enforcement agencies, engaging in threat response, are the equivalent of the police. They work to identify and catch the criminal that set the fire. DHS is the only agency with a critical role in asset and threat response.

PPD-41 also directs DHS to lead the effort to write the National Cyber Incident Response Plan (NCIRP). This plan will formalize the incident response practices that have been developed over the past few years and will in further detail clarify organizational roles, responsibilities, and actions to prepare for, respond to, and coordinate the recovery from a significant cyber incident. This plan will build upon the PPD and include the private sector and other levels of government.



Links:

- [PPD-41](#)
- [Annex](#)
- [White House fact sheet](#)
- [DHS Secretary Johnson’s statement](#)
- [PPD-41 Stakeholder Message](#)
- [Cyber Incident Reporting: A Unified Message For Reporting To The Federal Government](#)

### US-CERT Portal Moving to HSIN, Changing Name in Fall 2016

The U.S. Department of Homeland Security (DHS) has made the decision to consolidate all secure portal capabilities in a single platform, and that platform will be the [Homeland Security Information Network \(HSIN\)](#).

The HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information with streamlined collaboration and real-time communications throughout all homeland security mission areas.

In the next few months, the US-CERT Portal (NC4 Mission Center) will migrate all content to HSIN (including the

ICS-CERT compartment). This migration will provide significant functionality, features, and enhanced security, and it will enable greater customization and configuration for the communities (formerly compartments) that move to HSIN.

In addition, the new portal will be rebranded as the National Cybersecurity and Communications Integration Center (NCCIC) Portal to reflect the fact that the portal is a resource for all NCCIC organizations and stakeholders.

For more information on the HSIN Program, please visit the [HSIN page on the DHS website](#).

## CSET 8.0

ICS-CERT's Cybersecurity Evaluation Tool (CSET®) continues to grow and expand, helping asset owners maximize their cybersecurity investment and resources. ICS-CERT will release CSET Version 8.0 in September 2016. This new version of CSET is the most significant change to CSET in the last 4 years. This version includes additional assistance to help users select their standards, determine security assurance levels, and prepare for an assessment. It also includes four new standards: Health Insurance Portability and Accountability Act (HIPAA), Critical Security Controls (CSC), CCIs (Control Correlation Identifiers), and National Institute of Standards and Technology (NIST)

SP800-171. In addition to these new enhancements, ICS-CERT is offering additional training and assistance to help asset owners better use the tool.

On September 20th, at 11 a.m. MDT, the CSET team will hold a CSET webinar, available worldwide. The session will include an introduction to CSET, details on new changes and features in Version 8.0, information on how to best use the tool, and an open question and answer session. This webinar will train participants in basic and advanced CSET functionality and show them how using CSET can improve their organization's overall cybersecurity posture. For additional information on the scheduled CSET webinars, go to <https://cset.inl.gov/SitePages/Webinar.aspx>.

CSET is distributed freely with the intent that users can quickly determine their cybersecurity stance and priorities and focus their limited cybersecurity time and money on implementing controls and



mitigating vulnerabilities. With these new changes, the CSET development team hopes to reduce the amount of time that asset owners must spend researching what to do during an incident. Instead, these changes will allow them to quickly close cybersecurity gaps, implement security controls, and mitigate discovered issues. For additional information on CSET or to download a copy, go to <https://ics-cert.us-cert.gov/Assessments>. For defect reporting and feature request, go to <http://cset.inl.gov>.

### ICSJWG Fall 2016 Meeting Preview

The Industrial Control Systems Joint Working Group (ICSJWG) 2016 Fall Meeting is approaching quickly. This year's Fall meeting will be held in Fort Lauderdale, Florida, from September 13-15, at the Embassy Suites Fort Lauderdale 17th Street hotel

Confirmed Keynote Speakers:

- Billy Rios, Founder of WhiteScope
- Joel Langill, AECOM
- John Felker, Director of Operations, NCCIC, DHS
- Marty Edwards, Director, ICS-CERT, DHS

Meeting Highlights:

- Hands-On Technical Workshop and Training focused on Network Monitoring of ICS and Google Hacking/Shodan
- "Ask Me Anything" session with Marty Edwards
- Plenary panel sessions focused on Vulnerability Coordination and Research
- Back by Popular Demand: "Viewing Your Network Through the Eyes of an Attacker."

Additional information regarding the agenda, venue, and registration are available on the ICSJWG web site: <https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>.



## NCCIC team wins 1st Place at FIRST Conference in Seoul

In June, several members of US-CERT and ICS-CERT traveled to South Korea to attend the 28th Annual Forum for Incident Response and Security Teams (FIRST) Conference in Seoul. This annual conference brings forensic analysts, malware reverse engineers, vulnerability handlers and policy development professionals from around the world together from both government and private sectors.

The primary goal of the conference is to disseminate information on new incidents and about new techniques developed by incident responders and security tool developers. During the course of the conference, attending groups create networking pipelines between both individuals and organizations that lead to higher levels of cooperation between CERT teams around the world.

While at the conference, the ICS-CERT/US-CERT team competed in the Capture the Flag (CTF) event and won first place. This was the first time that ICS-CERT/US-CERT fielded a team for the competition, which included over 30 teams from around the world (including teams from Amazon and Netflix).



Members of the joint ICS-CERT/US-CERT team after winning the CTF contest at the 28th Annual FIRST Conference in Seoul, South Korea. Left to Right: Mark Bristow, Deputy Chief of NCCIC Incident Response; Kenneth Melton of US-CERT; Chris Butera, Chief of NCCIC Incident Response; and David Hudson of ICS-CERT's Advanced Analytical Laboratory (AAL).

## ICS-CERT Training Pursuing Status as Accredited Provider of Continuing Education Units

The ICS-CERT training team is currently working to become an Accredited Provider (AP) of Continuing Education Units (CEUs) through the International Association of Continuing Education and Training (IACET). As an AP, the team will be able to assign CEUs for training courses. The [CEU](#) is designed to:

- Provide a standard unit of measurement for continuing education and training,
- Quantify continuing education and training activities, and
- Accommodate for the diversity of providers, activities, and purpose in adult education.

Achieving [IACET AP status](#) will demonstrate that ICS-CERT has:

- Committed to a rigorous accreditation application and review process, involving extensive hands-on evaluation and verification,
- Benchmarked our policies and processes thoroughly against the ANSI/IACET Standard for Continuing Education and Training, and
- Engaged the expertise of instruction design professionals nationwide to make our continuing education and training the best it can be.



## Onsite Assessments Summary

# ICS-CERT Assessment Activity for July/August 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 July/August 2016, ICS-CERT conducted 21 onsite assessments across five sectors (Table 1). Of these 21 assessments, five were Cyber Security Evaluation Tool (CSET®) assessments, 10 were Design Architecture Review (DAR) assessments, and six 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, July/August 2016.

Assessments by Sector	July 2016	August 2016	July/August Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams		2	2
Defense Industrial Base			
Emergency Services		3	3
Energy		4	4
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems	2		2
Water and Wastewater Systems	6	4	10
<b>Monthly Totals</b>	<b>8</b>	<b>13</b>	<b>21 Total Assessments</b>

Table 2: Assessments by type, July/August 2016.

Assessments by Type	July 2016	August 2016	July/August Totals
CSET	2	3	5
DAR	4	6	10
NAVV	2	4	6
<b>Monthly Totals</b>	<b>8</b>	<b>13</b>	<b>21 Total Assessments</b>



## Recent Product Releases

### Alerts

[IR-ALERT-L-16-230-01](#) Navis WebAccess SQL Injection Exploitation, August 17, 2016

[ICS-ALERT-16-230-01](#) Navis WebAccess SQL Injection Vulnerability, August 17, 2016

### Advisories

[View Advisories Feed](#)

[ICSA-16-236-01A](#) Moxa OnCell Vulnerabilities, August 30, 2016

[ICSA-16-231-01](#) Navis WebAccess SQL Injection Vulnerability, August 18, 2016

[ICSA-16-224-01](#) Rockwell Automation MicroLogix 1400 SNMP Credentials Vulnerability, August 11, 2016

[ICSA-16-215-01](#) Moxa SoftCMS SQL Injection Vulnerability, August 02, 2016

[ICSA-16-215-02](#) Siemens SINEMA Server Privilege Escalation Vulnerability, August 02, 2016

[ICSA-16-208-01A](#) Siemens SIMATIC WinCC, PCS 7, and WinCC Runtime Professional Vulnerabilities (Update A), August 16, 2016

[ICSA-16-208-02](#) Siemens SIMATIC NET PC-Software Denial-of-Service Vulnerability, July 26, 2016

[ICSA-16-208-03](#) Siemens SINEMA Remote Connect Server Cross-site Scripting Vulnerability, July 26, 2016

[ICSA-16-173-03](#) Rockwell Automation FactoryTalk EnergyMetrix Vulnerabilities, July 26, 2016

[ICSA-16-196-01](#) Schneider Electric Pelco Digital Sentry Video Management System Vulnerability, July 14, 2016

[ICSA-16-196-02](#) Moxa MGate Authentication Bypass Vulnerability, July 14, 2016

[ICSA-16-196-03](#) Schneider Electric SoMachine HVAC Unsafe ActiveX Control Vulnerability, July 14, 2016

[ICSMA-16-196-01](#) Philips Xper-IM Connect Vulnerabilities, July 14, 2016

[ICSA-16-194-01](#) Tollgrade Smart Grid EMS LightHouse Vulnerabilities, July 12, 2016

[ICSA-16-194-02](#) GE Proficy HMI SCADA CIMPLICITY Privilege Management Vulnerability, July 12, 2016

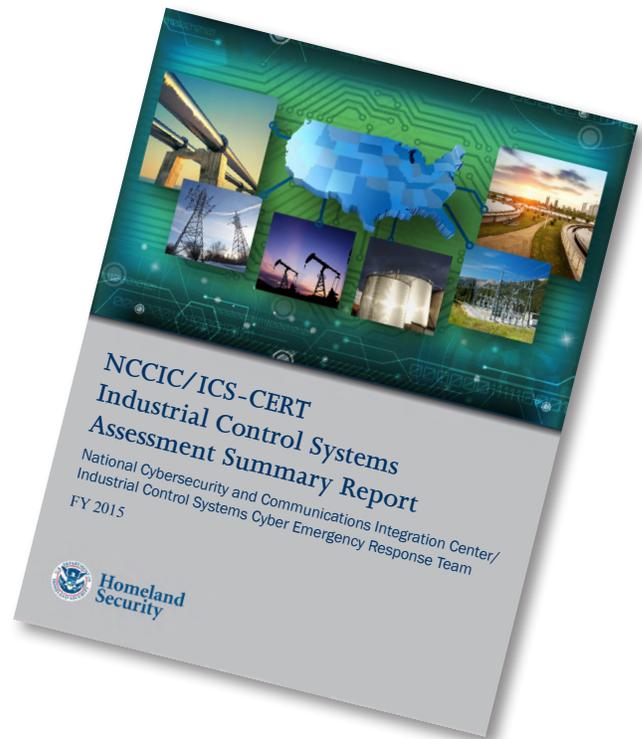
[ICSA-16-189-01](#) WECON LeviStudio Buffer Overflow Vulnerabilities, July 7, 2016

[ICSA-16-189-02](#) Moxa Device Server Web Console Authorization Bypass Vulnerability, July 7, 2016

[ICSA-16-187-01](#) Rexroth Bosch BLADEcontrol-WebVIS Vulnerabilities, July 5, 2016

### Other

[NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report](#), 8/4/16



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](mailto:ics-cert@hq.dhs.gov) or toll free at 1-877-776-7585.

## Researchers Assisting ICS-CERT with Products Published July/August 2016

ICS-CERT appreciates having worked with the following researchers:

- Independent researcher Maxim Rupp, ICSA-16-236-01A Moxa OnCell Vulnerabilities, August 30, 2016
- Cisco Talos, Cisco Systems, Inc.'s security intelligence and research group ICSA-16-224-01 Rockwell Automation MicroLogix 1400 SNMP Credentials Vulnerability, August 11, 2016
- Zhou Yu of Acorn Network Security, ICSA-16-215-01 Moxa Soft-CMS SQL Injection Vulnerability, August 02, 2016
- Security researcher rgod working with Trend Micro's Zero Day Initiative ICSA-16-215-02 Siemens SINEMA server Privilege Escalation Vulnerability, August 02, 2016
- Researchers Antonio Morales Maldonado of INNOTECH SYSTEM, Alexander Van Maele, and Tijl Deneut of Howest, ICSA-16-208-03 Siemens SINEMA Remote Connect Server Cross-site Scripting Vulnerability, July 26, 2016
- Independent researcher Maxim Rupp, ICSA-16-196-02 Moxa MGate Authentication Bypass Vulnerability, July 14, 2016
- Andrea Micalizzi, ICSA-16-196-03 Schneider Electric SoMachine HVAC Unsafe ActiveX Control Vulnerability, July 14, 2016
- Independent researchers Mike Ahmadi of Synopsys and Billy Rios of Whitescope LLC, ICSA-16-196-01 Philips Xper-IM Connect Vulnerabilities, July 14, 2016
- Ashish Kamble of Qualys, Inc., ICSA-16-194-01 Tollgrade Smart Grid EMS LightHouse Vulnerabilities, July 12, 2016
- Zhou Yu of Acorn Network Security, ICSA-16-194-02 GE Proficy HMI SCADA CIMPLICITY Privilege Management Vulnerability, July 12, 2016
- Independent security researchers Rocco Calvi and Brian Gorenc, working with Trend Micro's Zero Day Initiative WECON LeviStudio Buffer Overflow Vulnerabilities, July 7, 2016
- Independent researcher Maxim Rupp, ICSA-16-189-02 Device Server Web Console Authorization Bypass Vulnerability, July 7, 2016
- Independent researcher Maxim Rupp, ICSA-16-187-01 Rexroth Bosch BLADEcontrol-WebVIS Vulnerabilities, July 5, 2016



## Upcoming Events

### September 2016

ICSJWG 2016 Fall Meeting

**September 13-15**

Ft. Lauderdale, Florida

[Details and Registration](#)

### December 2016

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

**December 12-16**

Idaho Falls, Idaho

Registration will open on the week of  
September 19th.

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](mailto: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](mailto: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>.