November/December 2015

Homeland Security

ICS-CERT MONITOR

Contents

National Cybersecurity and Communications Integration Center

ICS-CERT

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

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

Contact Information

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

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

Report an ICS incident to ICS-CERT

Report an ICS software vulnerability

Get information about reporting

Joining the Secure Portal

ICS-CERT encourages US asset owners and operators to join the Control Systems Compartment of the US-CERT secure portal to receive up-to-date alerts and advisories related to industrial control systems (ICS) cybersecurity. To request a portal account, send your name, telephone contact number, email address, and company affiliation to ics-cert@hq.dhs.gov.

Downloading PGP/GPG Keys

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

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.

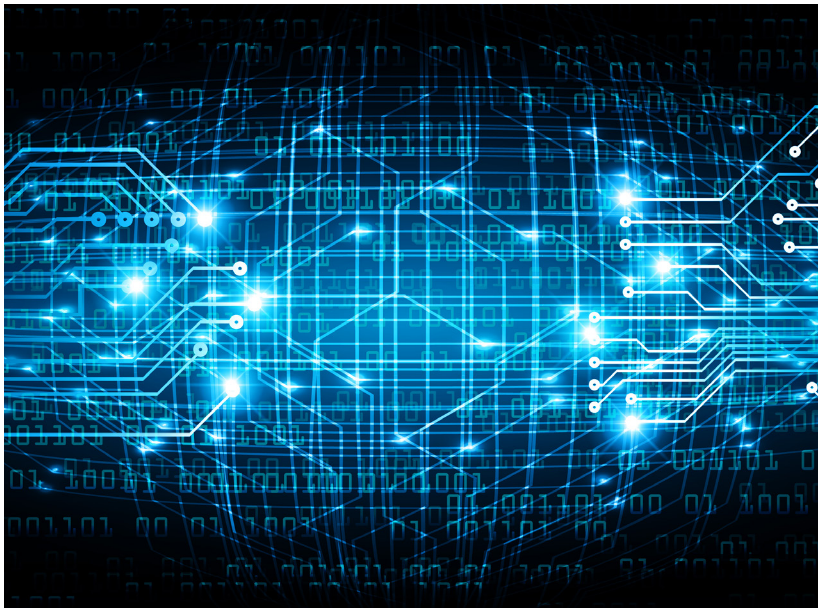
Incident Response Activity

Notable Incident

While the ICS-CERT Assessment team was assisting an asset owner with a Network Architecture Validation and Verification (NAVV) assessment, suspicious network traffic led them to call in the Incident Response team. Analysis of the log files and packet capture data determined that a system was infected with malware and was beaconing out to a suspicious IP address on the Internet. Working together, the Incident Response and Assessment teams made drive images to send back to the Advanced Analytical Lab (AAL) for processing. Preliminary mitigation information was provided to the entity to begin cleanup. Even though the infection vector wasn't found, this incident resulted in specific information used to strengthen the entity's security posture.

The skill of the Assessment group, which found the details of the infection, and teamwork with the Incident Response team and Advanced Analytical Lab led to a successful engagement with the asset owner. If you are an asset owner in need of assistance with an assessment, incident response, or malware analysis, visit https://ics-cert.us-cert.gov for more information.

> "Analysis of the log files and packet capture data determined that a system was infected with malware and was beaconing out to a suspicious IP address on the Internet."



Onsite Assessments Summary

ICS-CERT Assessment Activity for November/December 2015

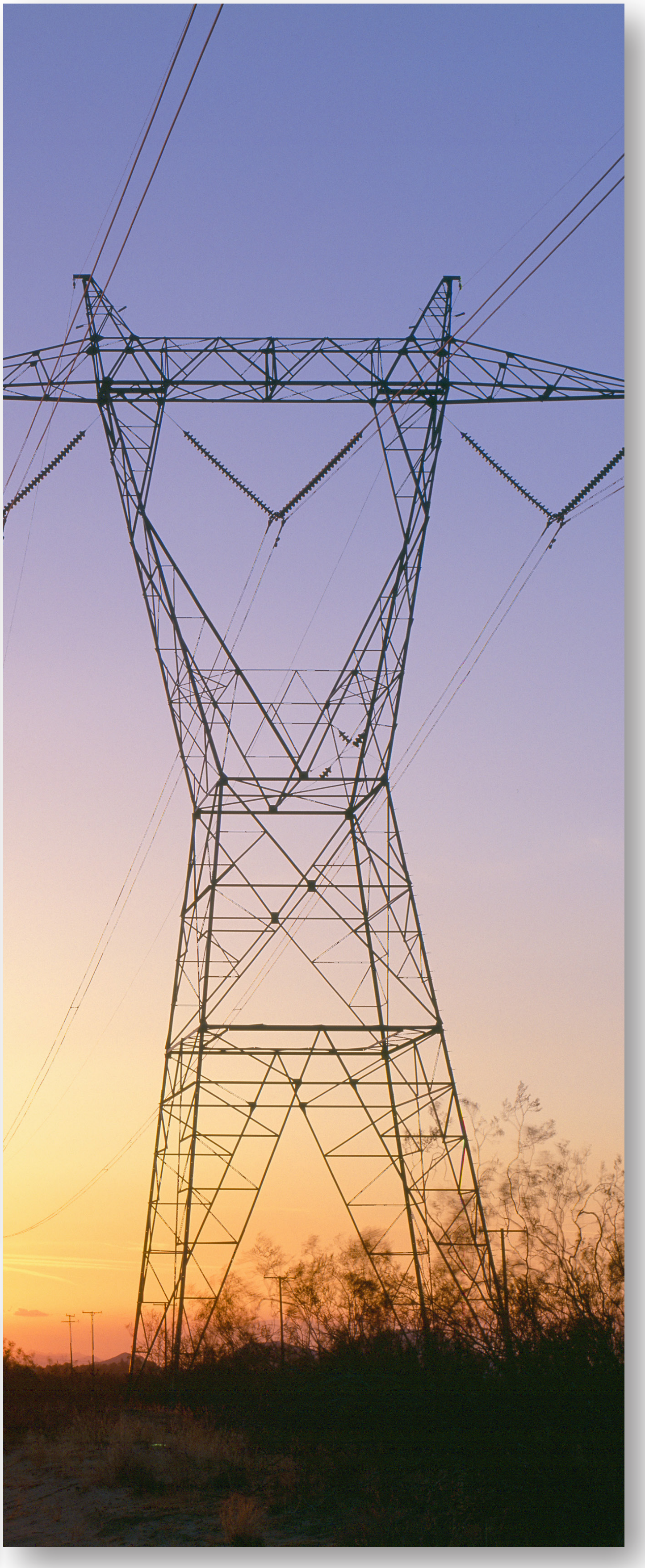
ICS-CERT conducts onsite cybersecurity assessments of industrial control systems (ICSs) to help strengthen the cybersecurity posture of critical infrastructure owners and operators and of ICS manufacturers. In November/December 2015, ICS-CERT conducted 18 onsite assessments across four sectors (Table 1). Of these 18 assessments, five were Cyber Security Evaluation Tool (CSET®) assessments, eight were Design Architecture Review (DAR) assessments, and five were Network Architecture Verification and Validation (NAVV) assessments (Table 2). For detailed information on ICS-CERT's CSET, DAR, and NAVV assessments, go to https://ics-cert.us-cert.gov/assessments.

Table 1. Assessments by sector, November/December 2015.

Assessments by Sector	November 2015	December 2015	November/ December Totals
Chemical			
Commercial Facilities		4	4
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	2		2
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology	1		1
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems		11	11
Monthly Totals	3	15	18 Total Assessments

Table 2. Assessments by type, September/October 2015.

Assessments by Type	November 2015	December 2015	November/ December Totals
CSET	1	4	5
DAR	1	7	8
NAVV	1	4	5
Monthly Totals	3	15	18 Total Assessments



Understanding Medical Vulnerabilities and ICS-CERT's Vulnerability Coordination Process

During the process of producing software products, vendors sometimes unintentionally create vulnerabilities that are later discovered and mitigated. ICS-CERT works with independent security researchers around the world who help to discover these vulnerabilities. The researchers who report product vulnerabilities to ICS-CERT are completely independent and are primarily interested in seeing vulnerabilities mitigated. ICS-CERT does not pay researchers for vulnerabilities they discover or direct researchers to explore specific vendors or products. Often vendors themselves will self-report security vulnerabilities to ICS-CERT as a means of more broadly disseminating vulnerability information to users of their products.

Over the past few years, there has been a notable upswing in medical device vulnerabilities reported to ICS-CERT. Because medical vulnerabilities are a relatively new area for cybersecurity, and because there are some concerns that releasing vulnerability information on medical devices could increase risk to the patient, ICS-CERT seeks to inform new vendors about the vulnerability coordination process and ICS-CERT's goals and objectives.

When ICS-CERT first notifies a vendor about a vulnerability, the vendor usually wants to know about the researcher who identified the vulnerability. All affected parties benefit by coordinating vulnerabilities with ICS-CERT. When researchers choose to work with ICS-CERT, vendors have the opportunity to create a product update and product owners have the opportunity to implement it before public disclosure of the vulnerability. Researchers benefit by receiving recognition from ICS-CERT for the work that they have done, and by simplifying the process of reporting a security vulnerability. Upon notification by a researcher, ICS-CERT notifies the vendor and asks them to validate the reported vulnerabilities. Vendors are also asked to test similar products for the reported vulnerabilities because it is common for manufacturers to share computer code across product lines.

Following vulnerability validation, ICS-CERT coordinates with the vendor during the mitigation process to provide additional information and recommendations, as necessary. ICS-CERT also works with the vendor to identify the release date for product updates and public notification. ICS-CERT works closely with both the independent security researcher and the vendor to develop mutually agreeable language for advisories. During this phase of the vulnerability coordination process, ICS-CERT strongly recommends that vendors provide regular updates on their progress and identify anticipated release dates for product updates to ICS-CERT. The most effective way to prevent premature vulnerability disclosures, once the vulnerability coordination process has started, is for vendors to share regular progress updates with the reporting researcher, the vast majority of whom just want to see the identified vulnerabilities fixed. With regular progress updates, ICS-CERT can more effectively manage the relationship with the researcher by showing that the vendor is responding to their concerns and is making progress toward mitigating the vulnerability.

It is common for newly contacted vendors to express some concerns about releasing a public advisory, and, as mentioned, some new vendors have questioned ICS-CERT's practice of releasing advisories about medical devices, citing concerns about the possibility of increasing risk to patients. The philosophy behind publicly disclosing vulnerability and mitigation information, however, is to help product users to protect themselves, which they cannot do if they do not know where they are vulnerable. ICS-CERT releases medical device advisories to provide actionable vulnerability and mitigation information to help organizations and patients to protect themselves. ICS-CERT is careful to limit the vulnerability information provided in advisories to a level sufficient to implement protection measures, but not enough to carry out an attack.

Vendors often ask if it is necessary to release an advisory even when all customers have been notified. It has been ICS-CERT's experience that many vendors find it challenging if not impossible to track every possible user of their products. It is common for companies to be bought or sold, change names, or resell equipment. ICS-CERT advisories, however, are broadly disseminated and improve the chances that more affected parties receive notification. The published vulnerabilities are also added to the National Vulnerability Database (NVD). NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. Other organizations, including the National Health Industry Sharing and Analysis Center (NH-ISAC), redistribute ICS-CERT alerts and advisories to their constituency to further broaden vulnerability information dissemination.

The goal of ICS-CERT vulnerability coordination is to protect and strengthen the Nation's 16 critical infrastructure sectors, including the Healthcare and Public Health Sector. ICS-CERT has determined that the best path to mitigating medical device vulnerabilities is the same as it is for each of the other sectors—by working with vendors to mitigate identified vulnerabilities in affected products and sharing information with the affected parties and the public.

ICS-CERT NEWS

ICS-CERT Fiscal Year 2015: Final Incident Response Statistics

In Fiscal Year (FY) 2015 (October 2014 through September 2015), ICS-CERT responded to 295 reported incidents involving critical infrastructure (CI) in the United States (see Figure 1). Sources of these incidents come from a combination of self-reporting to ICS-CERT, ISAC reports shared with ICS-CERT, third-party/researcher reports, and US Government sources. While these numbers provide some indication of the state of incidents against control systems and control systems asset owner/operators, they should not be considered comprehensive because not all parties choose to share incident information with ICS-CERT.

In FY 2015, the Critical Manufacturing sector had 97 reported incidents, representing 33 percent of the reported incidents for the fiscal year. This increase over previous years in the Critical Manufacturing sector is primarily related to a wide spread spear-phishing campaign that primarily targeted critical manufacturing companies along with limited targets in other sectors. In September 2015, ICS-CERT released ICS-ALERT-15-198-01AP regarding this activity. This alert is currently available to members of the ICS-CERT portal.

While sophisticated intrusions against asset owners persist, in FY 2015, ICS-CERT responded to a significant number of incidents enabled by insufficiently architected networks, such as ICS networks being directly connected to the Internet or to corporate networks, where spear phishing can enable access. It is uncertain if this was a change in targeting by adversaries, if these systems merely represented targets of opportunity, or if there is some other explanation. Regardless of cause, this reinforces the need for asset owners/operators to focus on security fundamentals such as those outlined in our DHS/FBI/NSA joint publication "Seven Steps to Effectively Defend Industrial Control Systems" and ICS-CERT's "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies."

Figure 2 provides a graph of the various techniques used in the intrusion attempts for the FY 2015 incidents. In 38 percent of cases in FY 2015, there were insufficient forensic artifacts to definitively identify an initial infection vector. ICS-CERT continues to stress the importance of network security monitoring (NSM) and host-based intrusion detection (HIDS) technologies, where the underlying systems can support it, to be deployed to better detect, respond to, and analyze incidents. Of the known initial infection vectors in FY 2015, spear phishing represented 37 percent of the total incidents. Being relatively easy to execute and demonstrably effective, spear phishing continues to be a common method of initial access against critical infrastructure targets.

A sharp decline in incidents was reported to ICS-CERT in network scanning and probing as compared to FY 2014. This decrease may not necessarily be representative of a reduction of frequency, but in

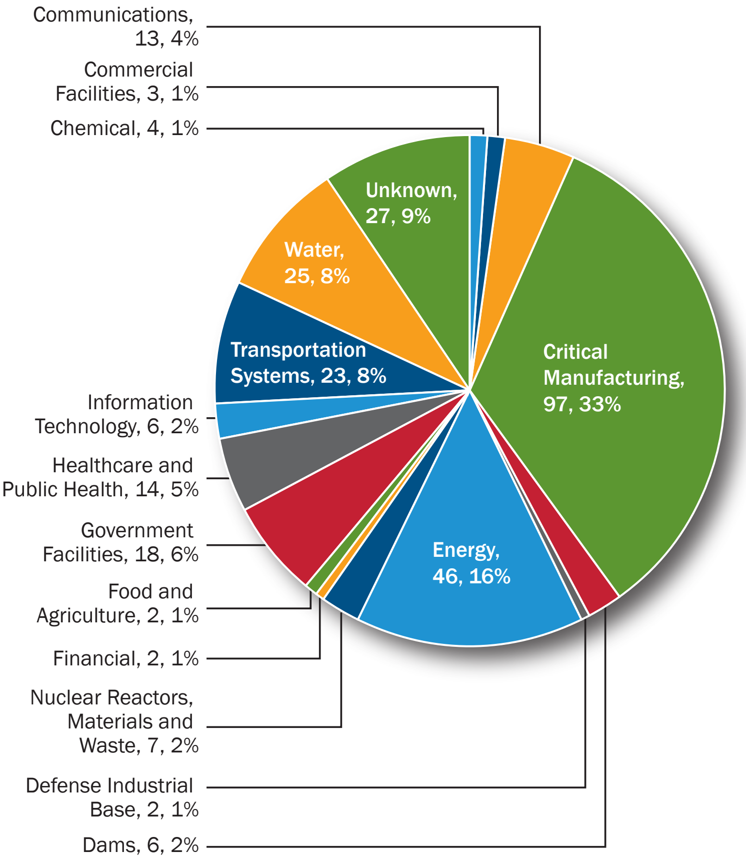


Figure 1. FY 2015 Incidents by Sector, 295 total.

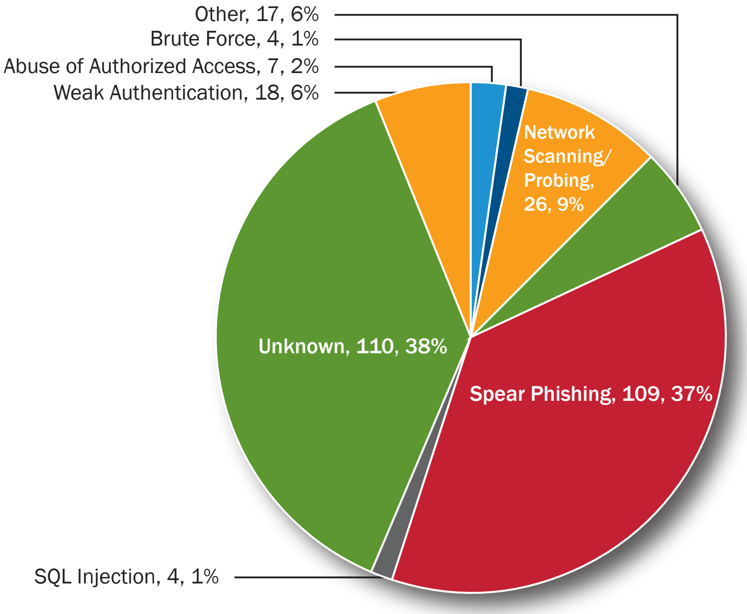


Figure 2. FY 2015 Incidents by Attempted Infection Vector, 295 total.

the maturation of individual organizations' ability to independently handle these low-level issues and a decrease in reporting or support requests to ICS-CERT.

In addition to an increase in the number of rudimentary intrusion vectors employed, ICS-CERT observed a significant number of incidents that were unsuccessful or successfully defended by asset owners in FY 2015. Approximately 69 percent of incidents had no evidence of successful intrusion into the asset owner's environment compared to 49 percent in FY 2014 (see Figure 3). Of concern, however, is the 12 percent of incidents in FY 2015 that had evidence of intrusion into the control system environment. This is up from 9 percent in FY 2014.

Direct reporting from CI stakeholders to ICS-CERT continues to provide the most immediate assistance in addressing cyber events. While reporting incidents to ICS-CERT is completely voluntary, CI asset owners gain access to ICS-CERT's unique capabilities and services at no cost. ICS-CERT specializes in working under the unique constraints of control systems and offers system owners assistance in identifying customized malware activity, conducting forensics on unique hardware/software configurations, and in developing recovery plans that maximize system availability. Organizations that choose to report to ICS-CERT can have their proprietary information kept confidential and protected from disclosure under the Protected Critical Infrastructure Information (PCII) Act. In addition to the direct benefits offered to the impacted organization, engagement with ICS-CERT also enables worldwide collaboration and analysis in developing defensive strategies that influence the ICS industry and contributes to national security.

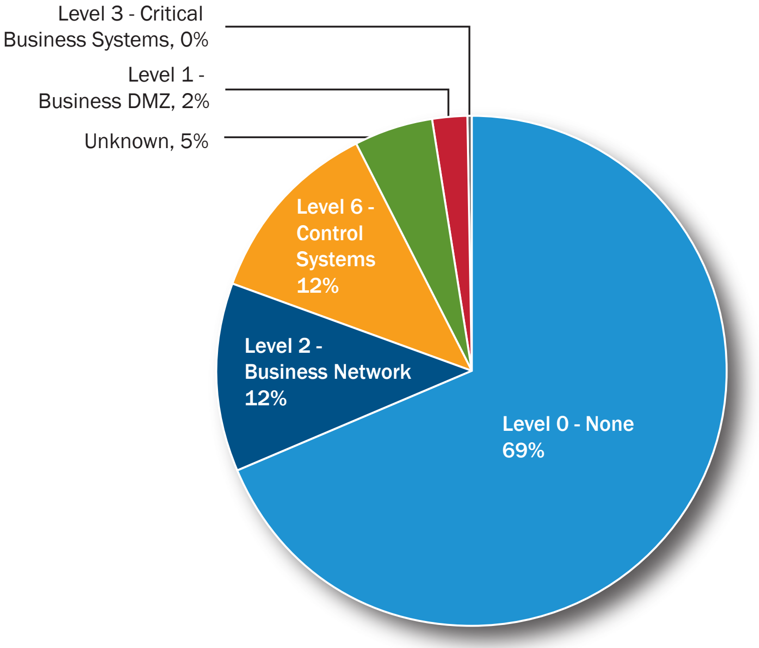
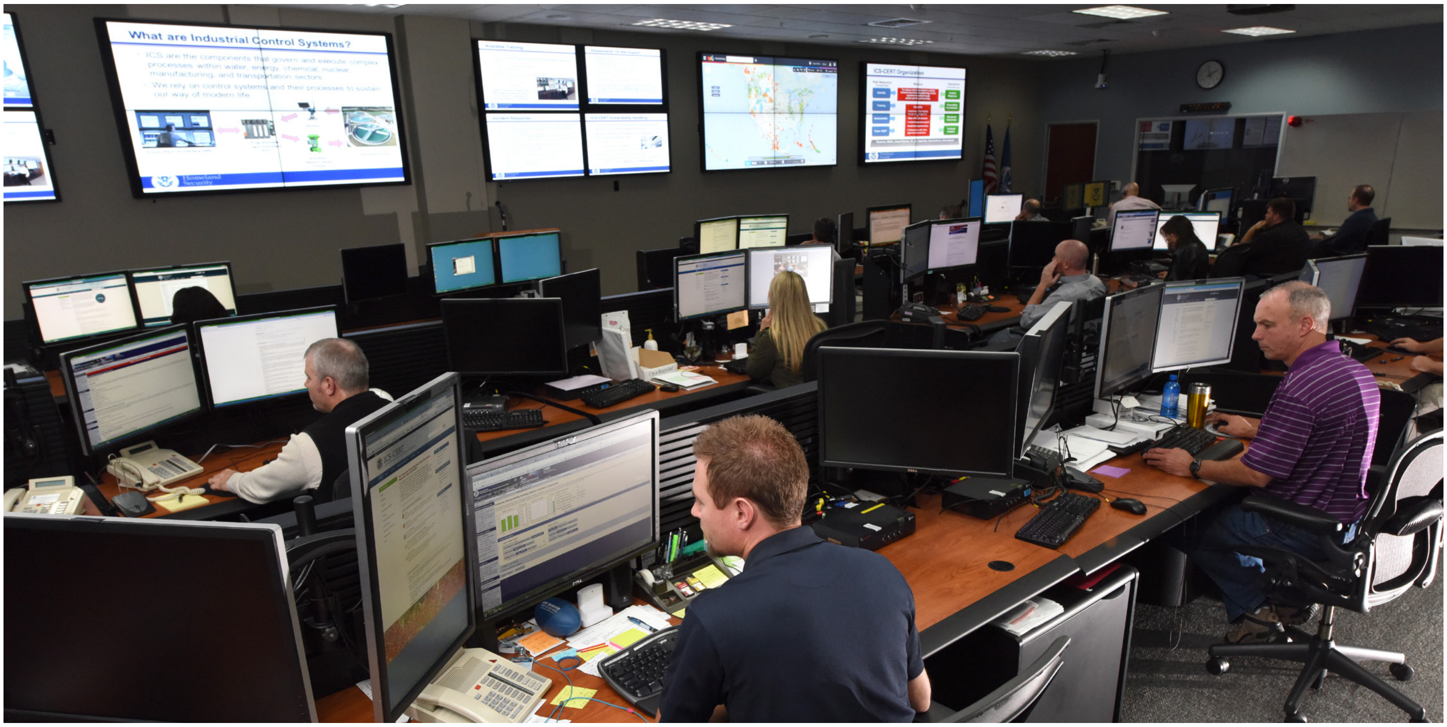


Figure 3. FY 2015 Observed Depth of Intrusion.



ICS-CERT FY 2015 Highlights

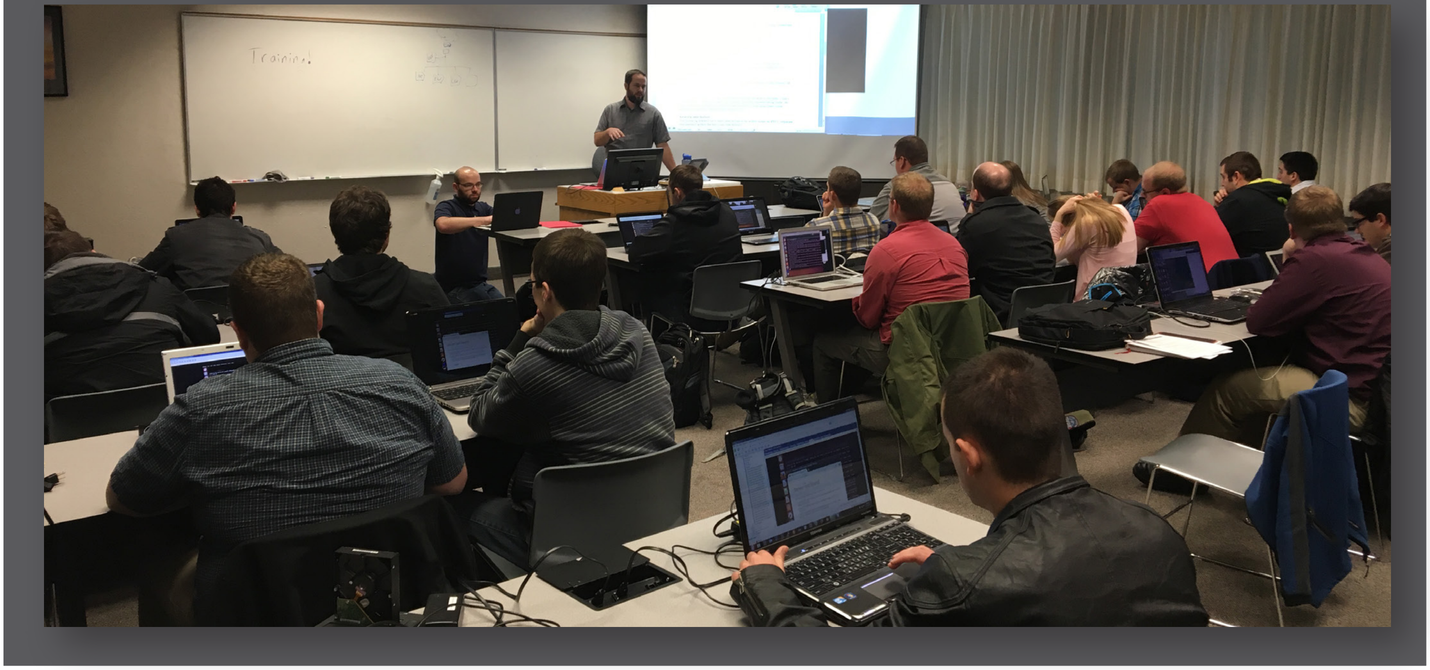
- **The President on NCCIC Watch Floor:** On January 13, 2015, the President of the United States visited the NCCIC watch floor to discuss his proposal for new cybersecurity legislation. In his 10-minute speech, the President emphasized that cyber threats pose an enormous challenge to the Nation and highlighted the need for greater trust and information sharing and collaboration between the government and the private sector.
- **ICS-CERT Runner-up for GISLA Award:** In May, ICS-CERT was announced as runner-up for the 12th Annual U.S. Government Information Security Leadership Awards (GISLA) Community Awareness Award. ICS-CERT received the runner-up GISLA award for its Action Campaign to educate CI asset owners about the Black Energy and Havex malware threat.
- **Incident Response:** In FY 2015, ICS-CERT responded to 295 cyber incidents. This represented a 20 percent increase over FY 2014. The Critical Manufacturing Sector nearly doubled to a record 97 incidents, becoming the leading sector for ICS-CERT in FY 2015. The Energy Sector had the second most incidents with 46 incidents, and the Water and Wastewater Systems Sector was third with 25.
- **Vulnerability Coordination:** ICS-CERT handled 321 vulnerabilities, a 39 percent increase over the 231 incidents handled in FY 2014. The vulnerability coordination team also reduced the average number of days to close a ticket from 108 days in 2014 to 55 days in 2015 and closed 76 percent of tickets that have been open over 365 days.
- **Assessments:** ICS-CERT conducted 112 onsite cybersecurity assessments across eight of the 16 CI sectors and in 20 states and Washington, D.C. Of these 112 assessments, 38 were CSET assessments, 46 were DAR assessments, and 28 were NAVV assessments. In August, the assessments team also released its annual report, "Industrial Control Systems Assessments FY 2014 Overview and Analysis."
- **Training:** The ICS-CERT training program upgraded the existing Virtual Learning Portal in August 2015. This upgrade better aligns the program with the federal guidelines for cloud-based applications, improves the graphical user interface, and reduces operational costs. The new VLP will also facilitate the program's goal of offering continuing education units.
- **CSET 6.2 and 7.0:** The CSET development team released two new versions of CSET in 2015. CSET 6.2 was released in January and CSET 7.0 was released in August. The latest version includes a new interface, new standards, improved functionality, and the ability to encrypt assessments files within CSET. In FY 2015, ICS-CERT distributed over 7,400 copies of CSET in 120 countries.
- **NCCIC/ICS-CERT Becomes Operational in Pensacola, Florida:** This year the NCCIC expanded watch floor operations in Pensacola, Florida, with the Senior Watch Officer for Pensacola beginning watch operations in September. Also in August, the ICS-CERT Production Chief was reassigned from Arlington, Virginia, to the Pensacola watch floor.
- **NCCIC elevated within DHS:** Because of its importance to the DHS cybersecurity mission, NCCIC was elevated within the DHS structure, with a direct incident reporting line to Secretary Jeh C. Johnson. As part of reorganization, John Felker was named as Director of Operations for NCCIC, with responsibility for day-to-day operations.

ICS-CERT Develops College Course in Cybersecurity

An ever-increasing need exists for college graduates to enter the workforce with basic cybersecurity skills to meet the challenges of protecting critical infrastructure from emerging and sophisticated cyber threats. In an effort to meet that need, ICS-CERT developed and piloted an upper-level cybersecurity course during the 2015 Fall Semester at Brigham Young University–Idaho (BYU–I) in Rexburg, Idaho. The 3-credit course was designed and taught by ICS-CERT personnel using the expertise, experience, and skills developed over years of services in the program. The course started with the basics of industrial control systems network operations and then provided students with concepts for securing these networks and segregating them from the Internet and corporate network environments. During the semester, students received hands-on experience in malware analysis, techniques for capturing forensic data, and incident response best practices—all valuable tools for any network administrator. The course also covered methods for protecting against destructive malware and provided exercises for detecting malware on a network.

One senior enrolled in the class said, "I didn't know I wanted to work with ICS security until I took this cybersecurity class." The course was designed to be presented in 3-hour sessions and included both lectures and demonstrations. ICS-CERT is planning to roll these modules into its advanced workforce development curriculum for use in training asset owners and operators in critical infrastructure.

Another senior from the class said, "I understood that ICS infrastructure existed, but I never knew how different the security strategies were for them. The class gave me incredible insight into a sector of security that needs much more awareness."



Industrial Control Systems Joint Working Group Meetings

We are excited to announce that the Industrial Control Systems Joint Working Group (ICSJWG) 2016 Spring Meeting will occur May 3-5, 2016, in Scottsdale, Arizona. Please save the date and watch for the call-for-abstracts and registration links that are coming soon. We look forward to seeing you in Scottsdale! When available, registration information will be posted here: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

Recent Product Releases

Advisories

ICSA-15-356-01 Siemens RUGGEDCOM ROX-based Devices NTP Vulnerabilities, 12/22/2015.

ICSA-15-202-03B Siemens RUGGEDCOM ROS and ROX-based Devices TLS POODLE Vulnerability, 12/22/2015.

ICSA-15-300-02A Infinite Automation Systems Mango Automation Vulnerabilities, 12/22/2015.

ICSA-15-351-01 Schneider Electric Modicon M340 Buffer Overflow Vulnerability, 12/21/2015.

ICSA-15-351-02 Motorola MOSCAD SCADA IP Gateway Vulnerabilities, 12/17/2015.

ICSA-15-351-03 eWON Vulnerabilities, 12/17/2015.

ICSA-15-349-01 Adcon Telemetry A840 Vulnerabilities, 12/15/2015.

ICSA-15-344-01A Advantech EKI Vulnerabilities, 12/15/2015.

ICSA-15-344-02 Open Automation Software OPC Systems NET DLL Hijacking Vulnerability, 12/10/2015.

ICSA-15-342-01A XZERES 442SR Wind Turbine Cross-site Scripting Vulnerability, 12/10/2015.

ICSA-15-342-02 LOYTEC Router Information Exposure Vulnerability, 12/08/2015.

ICSA-15-337-03 Pacom 1000 CCU GMS System Cryptographic Implementation Vulnerabilities, 12/08/2015

ICSA-15-337-01 SearchBlox File Exfiltration Vulnerability, 12/03/2015.

ICSA-15-309-02 Honeywell Midas Gas Detector Vulnerabilities, 12/03/2015.

ICSA-15-335-01 Saia Burgess Controls PCD Controller Hard-coded Password Vulnerability, 12/01/2015.

ICSA-15-335-02 Schneider Electric ProClima ActiveX Control Vulnerabilities, 12/01/2015.

ICSA-15-335-03 Siemens SIMATIC Communication Processor Vulnerability, 12/01/2015.

ICSA-15-328-01 Moxa OnCell Central Manager Vulnerabilities, 11/24/2015.

ICSA-15-295-01 Eaton's Cooper Devices Improper Ethernet Frame Padding Vulnerability, 11/24/2015.

ICSA-15-323-01 Tibbo AggreGate Platform Vulnerabilities, 11/19/2015.

ICSA-15-321-01 Exemys Web Server Bypass Vulnerability, 11/17/2015.

ICSA-15-274-02 Unitronics VisiLogic OPLC IDE Vulnerabilities, 11/13/2015.

ICSA-15-309-01 Advantech EKI Hard-coded SSH Keys Vulnerability, 11/05/2015.

Other

Seven Steps to Effectively Defend Industrial Control Systems, 12-29-15

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 2015

ICS-CERT appreciates having worked with the following researchers:

- Steven Seeley of Source Incite and Gjoko Krstic of Zero Science, ICSA-15-300-02A Infinite Automation Systems Mango Automation Vulnerabilities, 12/22/2015.
- David Atch of CyberX, ICSA-15-351-01 Schneider Electric Modicon M340 Buffer Overflow Vulnerability, 12/21/2015.
- Independent researcher Aditya K. Sood, ICSA-15-351-02 Motorola MOSCAD SCADA IP Gateway Vulnerabilities, 12/17/2015.
- Independent researcher Karn Ganeshen, ICSA-15-351-03 eWON Vulnerabilities, 12/17/2015.
- Independent researcher Aditya K. Sood, ICSA-15-349-01 Adcon Telemetry A840 Vulnerabilities, 12/15/2015.
- HD Moore of Rapid7, ICSA-15-344-01A Advantech EKI Vulnerabilities, 12/15/2015.
- Ivan Sanchez from Nullcode Team, ICSA-15-344-02 Open Automation Software OPC Systems NET DLL Hijacking Vulnerability, 12/10/2015.
- Independent researcher Maxim Rupp, ICSA-15-342-01A XZERES 442SR Wind Turbine Cross-site Scripting Vulnerability, 12/10/2015.
- Independent researcher Maxim Rupp, ICSA-15-342-02 LOYTEC Router Information Exposure Vulnerability, 12/08/2015.
- Oana Murarasu of Ixia, ICSA-15-337-01 SearchBlox File Exfiltration Vulnerability, 12/03/2015.
- Independent researcher Maxim Rupp, ICSA-15-309-02 Honeywell Midas Gas Detector Vulnerabilities, 12/03/2015.
- Independent researcher Artyom Kurbatov, ICSA-15-335-01 Saia Burgess Controls PCD Controller Hard-coded Password Vulnerability, 12/01/2015.
- Ariele Caltabiano, ICSA-15-335-02 Schneider Electric ProClima ActiveX Control Vulnerabilities, 12/01/2015.
- Lei ChengLin (Z-0ne) from the Fengtai Technologies' Security Research Team, ICSA-15-335-03 Siemens SIMATIC Communication Processor Vulnerability, 12/01/2015.
- Security researcher Andrea Micalizzi, ICSA-15-328-01 Moxa OnCell Central Manager Vulnerabilities, 11/24/2015.
- David Formby and Raheem Beyah of Georgia Tech, ICSA-15-295-01 Eaton's Cooper Devices Improper Ethernet Frame Padding Vulnerability, 11/24/2015.
- Security researcher Andrea Micalizzi, ICSA-15-323-01 Tibbo AggreGate Platform Vulnerabilities, 11/19/2015.
- Independent researcher Maxim Rupp, ICSA-15-321-01 Exemys Web Server Bypass Vulnerability, 11/17/2015.
- Steven Seeley of Source Incite, Fritz Sands of ZDI, and Andrea Micalizzi, ICSA-15-274-02 Unitronics VisiLogic OPLC IDE Vulnerabilities, 11/13/2015.
- Independent researcher Neil Smith, ICSA-15-309-01 Advantech EKI Hard-coded SSH Keys Vulnerability, 11/05/2015.

Follow ICS-CERT on Twitter: @icscert

Upcoming Events

February 2016

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

February 8–12

Idaho Falls, Idaho

Course Closed

March 2016

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

March 7–11

Idaho Falls, Idaho

Course Closed

April 2016

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

April 4–8

Idaho Falls, Idaho

Course description and registration

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

We Want to Hear From You

A key aspect of our mission is providing relevant and timely cybersecurity information products and services to industrial control system (ICS) stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we can work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to: ics-cert@hq.dhs.gov.

Reporting Incidents

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

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

What is the publication schedule for this newsletter?

ICS-CERT publishes the ICS-CERT Monitor when an adequate amount of pertinent information has been collected.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT Web page at: http://ics-cert.us-cert.gov.

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

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.