



**Homeland
Security**

ICS-CERT MONITOR



Contents

Incident Response Activity
Situational Awareness
Onsite Assessment Summary
ICS-CERT News
Recent Product Releases
Coordinated Vulnerability Disclosure
Open Source Situational
Awareness Highlights
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

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 U.S. 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

What Is Your Data Backup and Recovery Plan?

A water sector entity was hit with ransomware, which encrypted a large portion of customer data and a number of business systems. The entity did not pay the ransom amount and began recovery efforts shortly after the infection was noticed. Identified business systems were mostly virtual machines and were readily recovered from last known good backups. These backups had been recently captured, which facilitated fast recovery with a negligible amount of data loss.

The customer data had not been backed up as recently as the business systems. This led to a large gap between the last known good backup and current data sets. It is unknown if all the encrypted customer data will be recovered.

Backup and recovery schemas are vital to incident response planning. When planning backups, there are costs of storage, man-power, and data availability to consider. When should you capture a full backup? Should you supplement an infrequent full backup with an incremental or differential backup? On what schedule should you do so to avoid affecting operations? Has a recovery been exercised? How successful was the exercise? What gaps were identified?

These costs should be weighed against the value of the data being captured. How effectively will business operations continue with a gap in recovered data? Offsite storage is a good way to ensure the integrity of data, but it can add time to the recovery process and may make it harder to keep current data sets. The types of data considered vital and the frequency of the backup will drive a manageable recovery plan that fits the cost and risks of data loss.

Backup and recovery schemas are vital to incident response planning.



ICS-CERT Incident Handling

It's a Thursday evening on the ICS-CERT watch floor, and the daily tasks are winding down. This morning the incident response team held coordination meetings, leadership briefings, and made policy updates to reflect the latest threats. This afternoon, team members placed follow up calls to asset owners, updated paperwork, and finalized reports for previous incidents. The average day for an ICS-CERT incident handler isn't always exciting, but that can change at any moment.

Now it's nearly time to go home, and the quiet hum of servers is interrupted by the phone ringing. A worried voice on the other end is the system administrator of a small municipality water system. One of its pump station control panels has started streaming a massive amount of network traffic to an unusual IP address. There is a definite possibility that a hacker has gained access to the device, which thousands of people depend on for fresh, running water. Within minutes, the configuration of the network is conveyed to the ICS-CERT incident handler, and steps are taken to prevent malicious actions. The control interface must remain online, but address whitelists are instituted and communications are moved to nonstandard ports. A plan is developed, and, within days, forensics images of the controller and network hardware arrive at the ICS-CERT Advanced Analytics Laboratory (AAL). Through a process of reverse engineering the custom malware and analyzing the available

log files, ICS-CERT determines who the perpetrator was, how he got in, what data were accessed, and how to prevent the same intrusion at other facilities. Had it been necessary, a fly-away team would have been ready to go onsite and offer hands-on assistance.

ICS-CERT specializes in identifying and mitigating cyber attacks against highly specialized computer equipment. These systems aren't standard desktop workstations you buy from your local computer store, nor are the attackers using well-known computer viruses defendable with a common antivirus program. Industrial control systems (ICSs) represent the pinnacle of cyber targets, the highest value for both the attacker and the asset owner. Victory comes through the unified efforts of everyone from the engineer at the plant to the control system developer. ICS cybersecurity is not a plug-and-play solution—there aren't simple solutions that drop into a network and comprehensively protect critical assets. Instead, solid architectural design, thorough life-cycle management, active network monitoring, engaged incident response, and comprehensive mitigation techniques all contribute to a robust,

secure ICS infrastructure. When it comes to cybersecurity, it's a great day when consumers turn the handle or flip the switch, the water comes out or the light comes on, and they never have to consider what could have happened instead.

When it comes to cybersecurity, it's a great day when consumers turn the handle or flip the switch, the water comes out or the light comes on, and they never have to consider what could have happened instead.

secure ICS infrastructure. When it comes to cybersecurity, it's a great day when consumers turn the handle or flip the switch, the water comes out or the light comes on, and they never have to consider what could have happened instead.



Protected Critical Infrastructure Information Program

One of the main reasons that some industrial control system owners and operators are reluctant to contact ICS-CERT for incident response or cybersecurity assessments is the fear that their confidential information won't be properly protected. This, however, is why the Department of Homeland Security (DHS) established the Protected Critical Infrastructure Information (PCII) Program under the Critical Infrastructure Information Act of 2002 (CII Act).

The PCII Program created a new framework for protecting PCII that enables members of the private sector to voluntarily submit confidential information to DHS with the assurance that the information will be protected from public disclosure. PCII can only be accessed in accordance with strict safeguarding and handling requirements. All personnel who work on PCII are required to be trained, certified, and take annual refresher training. With the protections provided by the PCII program, owners and operators can be confident that sharing their information with the government will not expose sensitive or proprietary data. PCII is used strictly for homeland security purposes and is protected from the following:

- The Freedom of Information Act (FOIA),
- State, tribal, and local disclosure laws,
- Use in regulatory actions, and
- Use in civil litigation.

ICS-CERT's mission is to reduce risk to the Nation's critical infrastructure by strengthening control systems security and resilience through public-private partnerships. ICS-CERT provides efficient coordination of control systems-related security incidents and information sharing with federal, state, and local agencies and organizations, the intelligence community, and private sector constituents, including vendors, owners and operators,

and international and private sector CERTs. Information sharing among all these stakeholders benefits the entire industrial control systems community. The PCII program enables and enhances this information sharing by giving asset owners and operators confidence that they can safely share their information.

If you are interested in working with ICS-CERT, go to <https://ics-cert.us-cert.gov/>. You can be assured that the DHS's PCII program ensures that your sensitive and proprietary information will be protected.

For more information about PCII, go to <https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program> or send an email to pcii-info@dhs.gov.



Use Strong Passwords

Recently, the director of Gotham City Power became concerned about physical security at the plant. Because locks increase security, the director insisted that every door in the facility have a lock. In an effort to save money and reduce confusion, the purchasing agent decided to have all locks keyed to one pattern. The company safety officer insisted that emergency services personnel have access to a key to prevent the loss of life and property. And, finally, a key was placed outside the main door with instructions for what it opened. Now this scenario is obviously ridiculous, but it is not much different than leaving default passwords on your equipment!

If you feel confident in your company's password policy, take a moment and Google "Default password list" or "top 100 Passwords." If you find any of your passwords in either of these searches, know with 99.99 percent confidence that every script kiddy and wannabe hacker has an attack using that password.

There is only one proven method to prevent your password from being cracked: leave your device sealed in the box in which it was shipped. Otherwise, all passwords can be cracked. Given enough time and processing power, even the longest most random password can be cracked. To short circuit this process, you should change your passwords on a regular basis.

Conducting a forensic analysis requires backtracking through system logs. A properly configured logging system can collect system changes and identify who made the changes. For a log to enable user nonrepudiation, the log file must record certain data fields such as a unique user identifier/password pair. When multiple users operate under the same identifier/

password pair, it cancels nonrepudiation and reduces the effectiveness of a forensic analysis.

The easiest way to create a secure password is to use a random password generator. This type of software will do two things. First, it will provide you with a secure password that will significantly increase the time it takes for hackers to brute force their way into your system. Second, it will get you to write your password down. The first is a good thing, the second not so much.

Traditional password advice has changed, but not by much. A password should be at least 12 characters, which is long enough to reduce the chance of being cracked. It should include capital letters, lower-case letters, symbols, and numbers. It should not be a normal dictionary word. It should not be easily guessed. And, finally, it must be memorable enough so it doesn't need to be written down.

The best advice you can get about passwords is to treat them like your underwear:

- Change them on a regular basis—by changing your password, you reset the timer on when it will be cracked
- Never use somebody else's—using common passwords negates non-repudiation
- Don't show yours to anyone—create a memorable password and you won't need to write it down
- Make sure they don't have any holes—use symbols, numbers, upper and lower case letters, and at least 12 characters when creating a password.



BSides Conference

In early March, ICS-CERT team members attended the BSides SLC (Salt Lake City) security conference. BSides conferences are security "conferences by the community for the community." These conferences happen in cities all over the world throughout the year. BSides SLC saw an increase in the number of attendees this year with approximately 400 in attendance.

BSides SLC keynote addresses were given by BSides co-founder Jack Daniel and information security engineer and researcher Neil Wyler. Presentations included digital forensics and incident response, firmware analysis, building information security risk management programs, medical systems and device connectivity, and many others. Workshops provided a deeper dive into topics such as near field communications, open source intelligence analysis, and penetration testing.

ICS-CERT's mission is to raise awareness and guide a cohesive effort between government and industry to improve the cyber security posture of control systems within the nation's



critical infrastructure. At BSides SLC, ICS-CERT took advantage of outreach opportunities to engage with the community by building relationships and attending training to keep apprised of current trends and tools. ICS-CERT values the work being done by vendors, researchers, and asset owners to protect critical infrastructure.

Onsite Assessments Summary

ICS-CERT Assessment Activity for March/April 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 March/April 2016, ICS-CERT conducted 18 onsite assessments across six sectors (Table 1). Of these 18 assessments, four were Cyber Security Evaluation Tool (CSET®) assessments, seven were Design Architecture Review (DAR) assessments, and seven 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, March/April 2016.

Assessments by Sector	March 2016	April 2016	March/April Totals
Chemical	3		3
Commercial Facilities			
Communications		3	3
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	3	3	6
Financial Services			
Food and Agriculture			
Government Facilities		2	2
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems	2		2
Water and Wastewater Systems		2	2
Monthly Totals	8	10	18 Total Assessments

Table 2: Assessments by type, March/April 2016.

Assessments by Type	March 2016	April 2016	March/April Totals
CSET	2	2	4
DAR	3	4	7
NAVV	3	4	7
Monthly Totals	8	10	18 Total Assessments



Ukraine Action Campaign

The U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Department of Energy (DOE), and other Federal agencies have been actively working with the government of Ukraine to understand the December 23, 2015, attacks against Ukrainian power infrastructure. From March 31, 2016, to April 29, 2016, ICS-CERT and the FBI conducted unclassified in-person briefings and online webinars for asset owners and Federal, state, local, tribal and territorial government representatives to increase awareness of the threat and provide additional information. The briefing sessions provided details about the events surrounding the attack, techniques used by the threat actors, and strategies for mitigating risks and improving the cyber defensive posture of an organization. If you were unable to attend these briefings, the information is available in IR-ALERT-H-16-043-01BP, "Cyber-Attack Against Ukrainian



Critical Infrastructure," on the ICS-CERT secure portal. If your organization would like to request a briefing on this or any ICS-CERT topic, please email ICS-CERT@hq.dhs.gov and include the event details and the topics requested.

Recent Product Releases

Alerts

[ICS-ALERT-16-099-01B](#) Moxa NPort Device Vulnerabilities (Update B), April 27, 2016.

Advisories

[ICS-16-105-01](#) Sierra Wireless ACEmanager Information Exposure Vulnerability, April 14, 2016.

[ICS-16-105-02](#) Accuenergy Acuvim II Series AXM-NET Module Vulnerabilities, April 14, 2016.

[ICS-16-105-03](#) Ecava IntegraXor Vulnerabilities, April 14, 2016.

[ICS-16-103-01](#) Siemens Industrial Products glibc Library Vulnerability, April 12, 2016.

[ICS-16-103-02](#) Siemens SCALANCE S613 Denial-of-Service Vulnerability, April 12, 2016.

[ICS-16-103-03](#) Siemens Industrial Products DROWN Vulnerability, April 12, 2016.

[ICS-16-070-02](#) Honeywell Uniformance PHD Denial Of Service, April 12, 2016.

[ICS-16-096-01](#) Pro-face GP-Pro EX HMI Vulnerabilities, April 05, 2016.

[ICS-16-061-03](#) Eaton Lighting Systems EG2 Web Control Authentication Bypass Vulnerabilities, April 05, 2016.

[ICS-16-056-01](#) Rockwell Automation Integrated Architecture Builder Access Violation Memory Error, April 05, 2016.

[ICS-16-091-01](#) ICONICS WebHMI Directory Traversal Vulnerability, March 31, 2016.

[ICSMA-16-089-01](#) CareFusion Pyxis SupplyStation System Vulnerabilities, March 29, 2016.

[ICS-16-084-01](#) Cogent DataHub Elevation of Privilege Vulnerability, March 24, 2016.

[ICS-16-082-01](#) Siemens APOGEE Insight Incorrect File Permissions Vulnerability, March 22, 2016.

[ICS-16-077-01A](#) ABB Panel Builder 800 DLL Hijacking Vulnerability (Update A), March 17, 2016.

[ICS-16-075-01](#) Siemens SIMATIC S7-1200 CPU Protection Mechanism Failure, March 15, 2016.

[ICSA-16-070-01](#) Schneider Electric Telvent RTU Improper Ethernet Frame Padding Vulnerability, March 10, 2016.

[ICSA-16-063-01](#) Moxa ioLogik E2200 Series Weak Authentication Practices, March 03, 2016.

[ICSA-16-061-01](#) Schneider Electric Building Operation Automation Server Vulnerability, March 01, 2016.

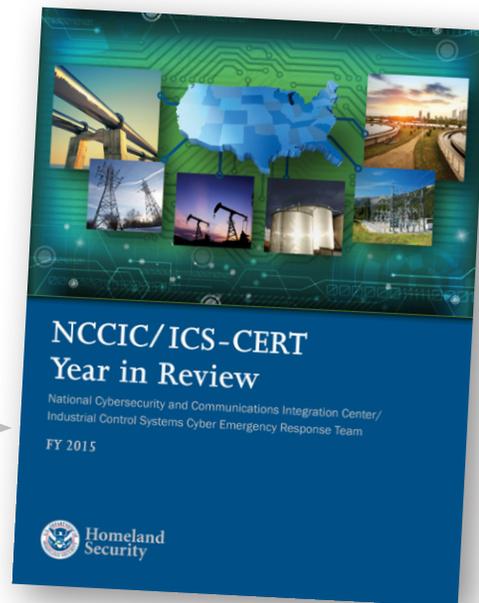
[ICSA-16-061-02](#) Rockwell Automation Allen-Bradley CompactLogix Reflective Cross-Site Scripting Vulnerability, March 01, 2016.

Other

[NCCIC/ICS-CERT Year in Review 2015](#), April 19, 2016.



Follow ICS-CERT on Twitter: [@icscert](#)



Coordinated Vulnerability Disclosure

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. Ideally, this coordinated disclosure process allows time for a vendor to develop and release patches, and for users to test and deploy patches prior to public vulnerability disclosure. While this process is not always followed for a variety of reasons, ICS-CERT continues to promote this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at ics-cert@hq.dhs.gov or toll free at 1 877 776 7585.

Researchers Assisting ICS-CERT with Products Published March / April 2016

ICS-CERT appreciates having worked with the following researchers:

- Reid Wightman of Digital Bond Labs, ICS-ALERT-16-099-01B Moxa NPort Device Vulnerabilities, April 27, 2016.
- Independent researcher Maxim Rupp, ICSA-16-105-01 Sierra Wireless ACEmanager Information Exposure Vulnerability, April 14, 2016.
- Independent researcher Maxim Rupp, ICSA-16-105-02 Accuenergy Acuvim II Series AXM-NET Module Vulnerabilities, April 14, 2016.
- Independent security researcher Marcus Richerson and Steven Seeley of Source Incite, working with Trend Micro's Zero Day Initiative, ICSA-16-105-03 Ecava IntegraXor Vulnerabilities, April 14, 2016.
- Zero Day Initiative (ZDI) and independent researcher Jeremy Brown, ICSA-16-096-01 Pro-face GP-Pro EX HMI Vulnerabilities, April 05, 2016.
- Independent researcher Maxim Rupp, ICSA-16-061-03 Eaton Lighting Systems EG2 Web Control Authentication Bypass Vulnerabilities, April 05, 2016.

- Ivan Sanchez from Nullcode Team, ICSA-16-056-01 Rockwell Automation Integrated Architecture Builder Access Violation Memory Error, April 05, 2016.
- Independent researcher Maxim Rupp, ICSA-16-091-01 ICONICS WebHMI Directory Traversal Vulnerability, March 31, 2016.
- Independent researchers Billy Rios and Mike Ahmadi in collaboration with CareFusion, ICSA-16-089-01 CareFusion Pyxis SuppLyStation System Vulnerabilities, March 29, 2016.
- Steven Seeley of Source Incite, ICSA-16-084-01 Cogent DataHub Elevation of Privilege Vulnerability, March 24, 2016.
- Ivan Sanchez from Nullcode Team, ICSA-16-077-01A ABB Panel Builder 800 DLL Hijacking Vulnerability (Update A), March 17, 2016.
- David Formby and Raheem Beyah of Georgia Tech, ICSA-16-070-01 Schneider Electric Telvent RTU Improper Ethernet Frame Padding Vulnerability, March 10, 2016.
- Independent researcher Aditya Sood, ICSA-16-063-01 Moxa ioLogik E2200 Series Weak Authentication Practices, March 03, 2016.
- Independent researcher Karn Ganeshen, ICSA-16-061-01 Schneider Electric Building Operation Automation Server Vulnerability, March 01, 2016.
- Independent researcher Aditya Sood, ICSA-16-061-02 Rockwell Automation Allen-Bradley CompactLogix Reflective Cross-Site Scripting Vulnerability, March 01, 2016.

Open Source Situational Awareness Highlights

Top news for posting on the ICS-CERT website

Survey results from Ponemon Institute shows one-third of C-level executives are never updated on cybersecurity incidents.

<http://www.esecurityplanet.com/network-security/34-percent-of-c-level-executives-are-never-updated-on-security-incidents.html>

Upcoming Events

June 2016

Cybersecurity for Industrial Control Systems Regional Training (4 days)

June 6 - 9

Bedford,
Massachusetts
(Due to venue restrictions, foreign national applications cannot be approved.)

[Course description and registration](#)

September 2016

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

Date TBD

Idaho Falls, Idaho

Course description and registration link will be posted when available

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 PClI 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>.