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.

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/ics-cert/

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.asc

Incident Response Activity

Notable Incident

In the course of incident response and assessments, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works with organizations that often lack adequate security measures, best practices/policies, documentation, and personnel. Cybersecurity can be a difficult proposition for the critical infrastructure community, and it is not the position of ICS-CERT to regulate or criticize the shortcomings of any organizations. Instead, ICS-CERT provides guidance and support to organizations in the form of assessment services and tools, subject matter expertise and analytic support, no-cost training, and other resources for use in strengthening cybersecurity against today's threats. Our mission is to assist critical infrastructure asset owners in reducing the risk of cyber attacks. The below incident scenario details an example of our onsite assistance for an organization dealing with a cyber-intrusion. The writeup is intended to provide insight into some common deficiencies that exist across many organizations today. ICS-CERT encourages organizations to make cybersecurity a priority and not wait until a significant incident has occurred.

A critical infrastructure asset owner recently engaged the ICS-CERT to evaluate the organization's control systems environment for possible advanced persistent threat (APT) activity. It had been discovered during previous incident response efforts that the bridge between the corporate and processing network had been compromised. Concerned about the integrity of the processing environment, the asset owner requested ICS-CERT support to analyze the systems for possible adversary activity and then, secondarily, evaluate the overall security posture.

ICS-CERT deployed both an incident response (IR) and assessment team to look for evidence of trespasser activity and to perform an architectural review of their security. Despite pre-planning measures, these efforts were hampered by insufficient asset management in the control systems environment that caused a significant delay in identifying systems for examination and evaluation. To compensate for incomplete documentation, the team instead led discussions and conducted reviews of available materials to determine undocumented systems and create an up-to-date representation of the network architecture.

The asset management issues also made it difficult to determine who had primary responsibilities for the various systems within the network. As the IR team interviewed the asset owner's personnel, it was evident that they lacked clearly defined roles and responsibilities for the systems within the control environment. This prolonged the response time for access requests, authorities, data, and information needed to support the incident response effort.

Host-based analysis efforts were also hampered due to a lack of forensic information that was not adequately preserved or maintained for the team. Because of this, ICS-CERT focused on network evaluation techniques identifying unusual use patterns in the ICS network. ICS-CERT also compared network-based findings against indicators collected from various sources in an attempt to identify adversary communications from any remnants.

While onsite the team quickly identified that the facility was using the same physical network cables and routing equipment for both networks, and that the only segmentation was the hard-coded IP addresses for the processing environment in a separate subnet from the corporate network. This meant that the two networks had essentially no segmentation. This segmentation issue was emblematic of the poor network visibility identified by the IR and assessment teams. The asset owner lacked capabilities to monitor network traffic and identify suspicious activity in the ICS and corporate enterprise. In addition, critical assets were left unmonitored with no physical security, leaving any employee the ability to tamper with critical systems undetected.

ICS-CERT provided a variety of recommendations and proposed a network re-design to heighten overall security posture and reduce the risk of future intrusion. These recommendations were provided at both the technical and policy levels and included guidance such as the following:

- Define and establish accurate asset management responsibilities and assign appropriate authorities
- Verify network architecture
- Deploy system patching and life cycle
- Create network segmentation
- Deploy physical security of critical assets
- Increase security operations staff and define mission roles and responsibilities
- Apply application whitelisting for approved applications and user authentication for remote access
- Deploy a security monitoring solution to ensure adequate visibility into the re-architected network.

ICS-CERT recommends that critical infrastructure asset owners review the best practices highlighted in the following documentation:

- Incident Handling: Preparing for Incident Analysis (https://ics-cert.us-cert.gov/sites/default/files/FactSheets/DHS_Cybersecurity_Incident_Handling_Brochure_20140113.pdf)
- Developing an Industrial Control Systems Cybersecurity Incident Response Capability (https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf).

ICS-CERT Assessment Activity for May/June 2015

In May/June 2015, ICS-CERT conducted 17 onsite assessments across 3 sectors (Table 1). Of these 17 assessments, 6 were Cyber Security Evaluation Tool (CSET®) assessments, 4 were Design Architecture Review (DAR) assessments, and 7 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, May/June, 2015.

Assessments by Sector	2015		May/June Totals
	May	June	
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	6	2	8
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	4	4	8
Monthly Totals	10	7	17 Total Assessments

Table 2. Assessments by type, May/June, 2015.

Assessments by Type	2015		May/June Totals
	May	June	
CSET	3	3	6
DAR	2	2	4
NAVV	5	2	7
Monthly Totals	10	7	17 Total Assessments

If You're Connected, You're Likely Infected!

Some asset owners may have missed the memo about disconnecting control system from the Internet. Our recent experience in responding to organizations compromised during the BlackEnergy malware campaign continues to bring to light this major cybersecurity issue—**Internet connected industrial control systems get compromised**. All infected victims of the BlackEnergy campaign had their control system directly facing the Internet without properly implemented security measures.

The BlackEnergy campaign took advantage of Internet connected ICS by exploiting previously unknown vulnerabilities in those devices in order to download malware directly into the control environment. Once inside the network, the threat actors added remote access tools, along with other capabilities to steal credentials and collect data about the network. With this level of access, the threat actor would have the capability to manipulate the control system.

There is, however, good news—simple and effective ways to improve your network defenses are available.

Isolate Your ICS Network from the Internet

Operators must isolate ICS networks from the Internet using reliable defensive measures and sound authentication requirements (strong user name and passwords). The majority of organizations that ICS-CERT notifies about Internet-connected control systems are not even aware that they are directly accessible. Most have assumed that they are securely configured or that their systems integrators have added proper security measures such as a firewall or VPN. In addition, many do not realize that there are publicly available tools, such as SHODAN, that can be easily used to discover connected control systems, making them an easy target for malicious activity.

An air-gapped control system is always the most secure. However, if you require remote access to your control systems environment, consider applying different levels of access: monitoring only (read) versus full control (write). Not everyone needs access to controlling the process. For some, "monitoring only" rights are adequate with no capabilities to make changes to the process. Access to the control system from the internal business network should also be limited and controlled using proven techniques for limiting access and data flow.

Limit and Secure the Use of Remote Access to Your Control System Environment

Take defensive measures to minimize the risk of exploitation from malicious cyber campaigns by managing remote access policies and processes. Specifically, ICS-CERT recommends that organizations do the following:

- Locate control system networks and devices behind firewalls and isolate them from the business network
- Work with your systems integrator or network administrator to review all remote access points within your network to identify potentially vulnerable Internet connections
- If you require remote access, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices
- Remove, disable, or rename any default system accounts wherever possible
- Implement policies requiring the use of strong passwords
- Log and monitor failed logon attempts to detect brute forcing activity
- Monitor the creation of administrator level accounts by third-party vendors.

Assign a Manager Responsible for Cybersecurity

Is someone in your organization assigned to be in charge of cybersecurity? ICS-CERT recommends that organizations assign a manager dedicated to develop, implement, and monitor security policies and procedures. This manager ensures that the organization trains and qualifies its employees. Organizations need regular assessments to identify gaps and make adjustments. Security is not a one-time effort, but rather a process of continuous improvement since the threat is always changing. It requires constant attention to identify and reduce emerging risks.

Implement Best Practices for Cybersecurity

Has your cybersecurity manager implemented the recommended best practices for a sound cyber defense? ICS-CERT provides reference materials and resources for critical infrastructure asset owners to assist with continuous improvement. The ICS-CERT web site contains a wealth of information products and reference materials that provide concepts for building defense-in-depth protections into your networks. There are also reference materials with recommendations for managing remote access to control system networks. The National Institute of Standards and Technology (NIST) Special Publication 800-82, "Guide to Industrial Control Systems Security," is also an excellent resource for building your cybersecurity program.

Incident Response Information and Services are Available

ICS-CERT provides a variety of resources to critical infrastructure asset owners to assist them in responding to a cyber event or intrusion. Our team can provide onsite incident response assistance, digital media and malware analysis in our analytical lab, and assist in the development of strategies for improving cyber defenses. We can also provide cybersecurity assessments to help identify security gaps in your policies, practices, and network configuration.

ICS-CERT also provides up-to-date security information concerning the threat landscape through alerts and advisories posted to our web site (ics-cert.us-cert.gov) and secure portal. Asset owners and operators of critical infrastructure, as well as those involved in the protection of those networks, can apply for a portal account by emailing ics-cert@hq.dhs.gov. Please include your company affiliation and company email address.

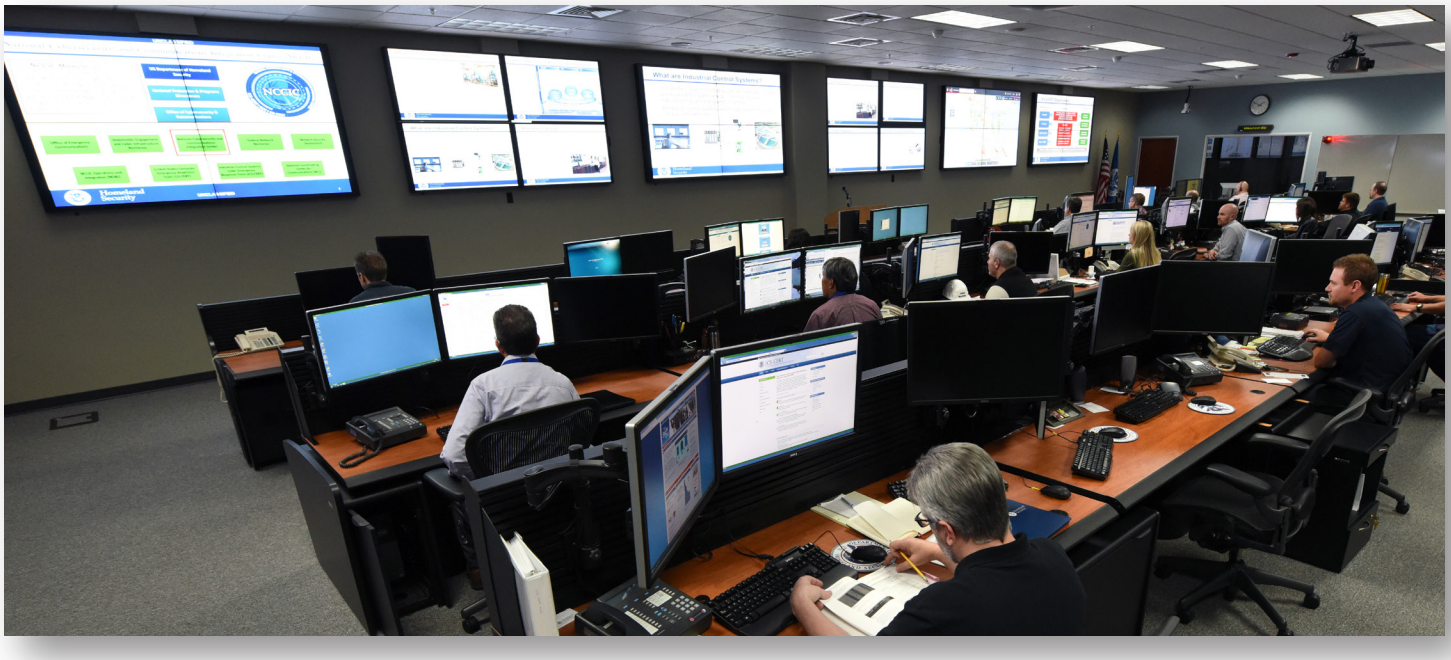
One More Thing

We want to hear from you. Please let us know if you have experienced a cyber intrusion or anomalous activity on your network.

Reporting is completely voluntary when working with ICS-CERT. However, your information is extremely useful for understanding the threat landscape that includes the techniques adversaries are using, types of malware, possible intent of campaigns, and sectors targeted. Reporting to ICS-CERT allows for the correlation of incident activity and has led to the discovery of campaigns aimed at certain sectors or groups. Moreover, the ICS-CERT anonymizes reports (to protect the reporting organization) and shares the analytically relevant data such as an attacker's IP address, command and control domains, malware, time stamps, email address and header information, and other data with the rest of the critical infrastructure community to alert them of malicious activity. Prompt and detailed reporting can lead to early detection and prevent incidents from occurring against the nation's critical infrastructure.

You can find out more about what, how, and why you should report your incidents to ICS-CERT at https://ics-cert.us-cert.gov/Report-Incident.

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



Using YARA for Malware Detection

When ICS-CERT included a YARA rule in one of its recent malware advisories, many network defenders called in asking "what is it and how do I use it?"

The effective sharing of intelligence to identify malware has always been a challenge for those working to protect information technology (IT) and industrial control systems networks. Traditional hash-based indicators are often not effective with sophisticated attacker groups and automated malware creation toolkits. Hash-based indicators look for exact matches; however, with one simple change of the malware, the indicator no longer works. Defenders can more successfully find malicious files if they focus on identifying malware families (groups of malware that share common code, but are not completely identical) instead of finding exact matches. YARA is a tool that specializes in this type of matching, and has grown to become a standard across the malware analysis community.

YARA is a very popular open-source and multi-platform tool (it works with most hosts running Windows, Linux, or Mac operating systems) that provides a mechanism to exploit code similarities between malware samples within a family. The signature files support the documentation of both byte-sequences and string matches that occur in the malware, as well as logic operators that support very robust and precise conditions to reduce the incidence of receiving false positives. ICS-CERT and other organizations use these signatures to disseminate the intelligence needed by asset owners to defend their networks. For example, the "blackenergy_v3.yara" file included in the Black Energy Alert is a signature file that tells the software what byte-sequences and/or strings on which to alarm. If it finds a match, it will then report to the user. YARA is host based, so users will need to execute the tool via an IT administration tool or manually on each host that they choose to examine. Users should be aware that the application will be analyzing every file in the path that they direct it to examine, so there may be some performance impact to the machine based on the available system resources.

You can download the YARA software and learn more about the tool at http://plusvic.github.io/yara/. If you deploy this to a Windows machine, you can use links on this page to download the precompiled binaries. Then you can simply unzip the downloaded Zip Archive and use a command line similar to this:

C:\<Path to Unzipped Archive>\yara32.exe -r <Path to blackenergy_v3.yara File> <Path to whatever you want to scan>

Note: You must have admin rights if you wish to scan a whole system.

The "-r" tells the program to recursively search the directories starting from the provided path.

Example:

C:\>yara32.exe -r c:\blackenergy_v3.yara c:

This example will search the entire "C" drive for anything that matches the signatures provided in the file "blackenergy_v3.yara." This command should be run as an administrator. If there is a hit on the signature, the output will include a line similar to the following:

Black Energy <Path to Suspicious File>

Using the freely available YARA tool, defenders are better able to leverage the intelligence available to them, and it also gives them a means of capturing data from their own incident response efforts, which they can use for the tracking of previous threats and for sharing threat information with others.

ICS-CERT Fiscal Year 2015: Mid-Year Statistics

In the first half of FY 2015 (October 2014 through April 2015), ICS-CERT responded to 108 cyber incidents impacting critical infrastructure in the United States (see Figure 1). As in previous years, the energy sector continues to lead all others with the most reported incidents. The water and critical manufacturing sectors also had notable percentages of incident reported to ICS-CERT, with 19 percent and 18 percent respectively.

Incident reporting is slightly below the pace for FY 2014. Of greater concern to ICS-CERT and DHS is the lower percentage of reporting directly by asset owners (see Figure 2). Just over one-quarter of the total reported incidents to ICS-CERT are coming directly from owners and operators, while federal partners, researchers, and open source media are the primary sources of reported incidents. In several cases, internal DHS analysis of data obtained through our partnerships in the cybersecurity community helped to uncover new incidents.

While reporting incidents to ICS-CERT is completely voluntary, we continue to encourage critical infrastructure stakeholders to contact us for assistance in responding to a malicious cyber event. We offer many services that are provided at no cost and will assist your organization in determining the depth of an intrusion as well as developing strategies for clean-up and recovery. The reported information is kept confidential and protected from disclosure under the PCII Act. Your information is extremely useful for understanding the current threats facing critical infrastructure and developing defense strategies that can benefit others in reducing cyber risks to our nation.

Figure 3 provides a graph of the various techniques used in the intrusions attempts for the mid-year 2015 incidents. Spear-phishing continues to be an often used method of attack, since it is relatively easy to execute and remains effective. Organizations should continue to emphasize, through training and awareness programs, the importance of not opening links in emails from unknown entities. Weak Authentication intrusions are often related to a lack of network segmentation and strong logon requirements for the control system environment. Once an intruder has penetrated the corporate network, they are often able to move laterally into the control system environment if strong authentication requirements are not in place. Network scanning and SQL injection attempts also remain popular as threat actors look for opportunities to exploit security vulnerabilities in web applications. Asset owners should ensure their network defensive measures address the weaknesses that are exploitable via these popular intrusion techniques.

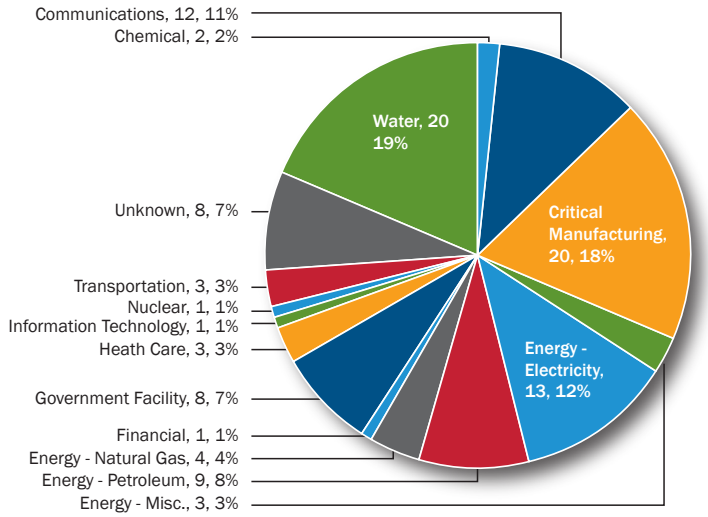


Figure 1. FY 2015 Mid-Year Incidents by Sector (108 total).

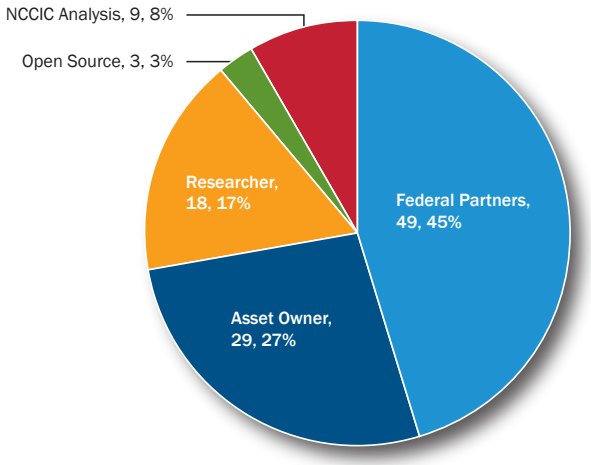


Figure 2. FY 2015 Mid-Year Incidents by Reporting Source (108 total).

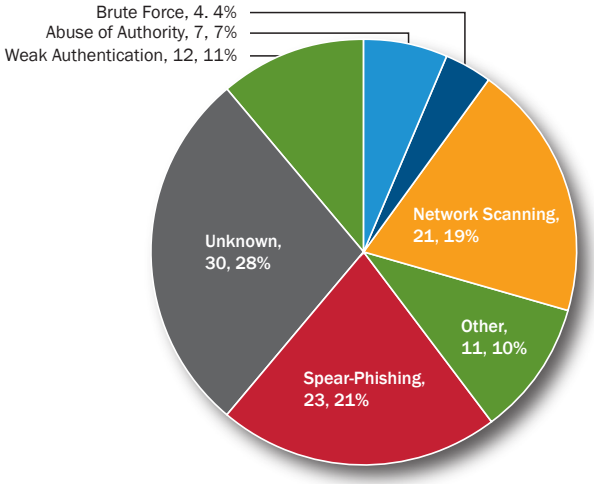


Figure 3: FY-2015 Mid-Year: Attempted Infection Vector.

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 critical infrastructure asset owners about the Black Energy and Havex malware threat.

As part of this Action Campaign, ICS-CERT provided both onsite and remote assistance to various critical infrastructure companies to perform forensic analysis of their control systems and conducted a deep dive analysis into both Havex and Black Energy malware. ICS-CERT partnered with the FBI to conduct classified and unclassified briefings for private sector critical infrastructure stakeholders across the country. From December 1st–11th, teams from ICS-CERT and the FBI traveled to 15 cities across the United States. In total, nearly 1,600 participants involved in the protection of critical infrastructure across all 16 sectors attended the briefings.

GISLA awards are given by the International Information System Security Certification Consortium, Inc. $(ISC)^2$, which is global organization providing educa tion and certification for security professionals. The $(ISC)^2$ U.S. GISLA program recognizes "the ongoing commitment of individuals whose initiatives, processes and projects have led to significant improvements in the security posture of a department, agency or the entire federal government." The Community Awareness award is a "project represented by U.S. federal, state or local information security personnel who have significantly contributed to building or broadening security awareness in the local community within the last 12 months."

Industrial Control Systems Joint Working Group

Spring 2015 Meeting Recap

The Spring 2015 Industrial Control Systems Joint Working Group (ICSJWG) Meeting was held June 23–24, 2015, at the Wilbur J. Cohen Building, 330 Independence Avenue SW, Washington, D.C., and covered a wide variety of topics in plenary presentations, panel discussions, and demonstrations. This ICSJWG meeting brought together asset owners and operators, government professionals, vendors, systems integrators, and academic professionals to discuss pressing issues across all of our critical infrastructure sectors. The Spring Meeting also featured a Q&A session with Director Marty Edwards and a classified threat briefing.

Fall 2015 Meeting

We are pleased to announce that the Fall 2015 ICSJWG Meeting will take place in Savannah, Georgia, on October 27–29. This meeting will feature multiple venues and formats for ICSJWG members to present their work with industrial control systems. When available, additional information and registration will be posted here: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

Recent Product Releases

Advisories

ICSA-15-176-01 Siemens Climatix BACnet/IP Communication Module Cross-site Scripting Vulnerability, 6/25/2015.

ICSA-15-176-02 PACTware Exceptional Conditions Vulnerability, 6/25/2015.

ICSA-15-169-01 Wind River VXWorks TCP Predictability Vulnerability in ICS Devices, 6/18/2015.

ICSA-15-169-02 Schneider Electric Wonderware System Platform Vulnerabilities, 6/18/2015.

ICSA-15-167-01 GarrettCom Magnum Series Devices Vulnerabilities, 6/16/2015.

ICSA-15-162-01A RLE Nova-Wind Turbine HMI Unsecure Credentials Vulnerability, 6/11/2015.

ICSA-15-161-01 Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities, 6/10/2015.

ICSA-15-125-01B Hospira LifeCare PCA Infusion System Vulnerabilities, 6/10/2015.

ICSA-15-160-01 N-Tron 702W Hard-Coded SSH and HTTPS Encryption Keys, 6/9/2015.

ICSA-15-160-02 Sinapsi eSolar Light Plaintext Passwords Vulnerability, 6/9/2015.

ICSA-15-155-01 XZERES 442SR Wind Turbine CSRF Vulnerability, 6/4/2015.

ICSA-15-153-01 Beckwith Electric TCP Initial Sequence Vulnerability, 6/2/2015.

ICSA-15-153-02 Moxa SoftCMS Buffer Overflow Vulnerability, 6/2/2015.

ICSA-15-148-01 IDS RTU 850 Directory Traversal Vulnerability, 5/28/2015.

ICSA-15-132-02 Rockwell Automation RSView32 Weak Encryption Algorithm on Passwords, 5/26/2015.

ICSA-15-141-01 Schneider Electric OFS Server Vulnerability, 5/21/2015.

ICSA-15-111-01 Emerson AMS Device Manager SQL Injection Vulnerability, 5/21/2015.

ICSA-14-202-01A OleumTech WIO Family Vulnerabilities, 5/21/2015.

ICSA-15-132-01 OSIsoft PI AF Incorrect Default Permissions Vulnerability, 5/12/2015.

ICSA-15-111-02 Rockwell Automation RSLinx Classic Vulnerability, 5/7/2015.

Follow ICS-CERT on Twitter: @icscert

Open Source Situational Awareness Highlights

Data Theft The Goal Of BlackEnergy Attacks On Industrial Control Systems, Researchers Say

2015-05-28

http://www.darkreading.com/endpoint/data-theft-the-goal-of-blackenergy-attacks-on-industrial-control-systems-researchers-say/d/d-id/1320599?_mc=RSS_DR_EDT&utm_source=dlvr.it&utm_medium=twitter

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 May/June 2015

ICS-CERT appreciates having worked with the following researchers:

- Ivan Sanchez from Nullcode Team, ICSA-15-176-02 PACTware Exceptional Conditions Vulnerability, 6/25/2015.
- Raheem Beyah, David Formby, and San Shin Jung of Georgia Tech, via a research project partially sponsored by the Georgia Tech National Electric Energy Testing Research and Applications Center, ICSA-15-169-01 Wind River VXWorks TCP Predictability Vulnerability in ICS Devices, 6/18/2015.
- Ivan Sanchez of WiseSecurity Team, ICSA-15-169-02 Schneider Electric Wonderware System Platform Vulnerabilities, 6/18/2015.
- Ashish Kamble of Qualys Security and Eireann Leverett, ICSA-15-167-01 GarrettCom Magnum Series Devices Vulnerabilities, 6/16/2015.
- Independent researcher Maxim Rupp, ICSA-15-162-01A RLE Nova-Wind Turbine HMI Unsecure Credentials Vulnerability, 6/11/2015.
- Independent researcher Billy Rios, ICSA-15-161-01 Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities, 6/10/2015.
- Independent researcher Billy Rios, ICSA-15-125-01B Hospira LifeCare PCA Infusion System Vulnerabilities, 6/10/2015.
- Independent researcher Neil Smith of (ZeroFox) Riskive Security, ICSA-15-160-01 N-Tron 702W Hard-Coded SSH and HTTPS Encryption Keys, 6/9/2015.
- Independent researcher Maxim Rupp, ICSA-15-160-02 Sinapsi eSolar Light Plaintext Passwords Vulnerability, 6/9/2015.
- Independent researcher Maxim Rupp, ICSA-15-155-01 XZERES 442SR Wind Turbine CSRF Vulnerability, 6/4/2015.
- Raheem Beyah, David Formby, and San Shin Jung of Georgia Tech, via a research project partially sponsored by the Georgia Tech National Electric Energy Testing Research and Applications Center, ICSA-15-153-01 Beckwith Electric TCP Initial Sequence Vulnerability, 6/2/2015.
- HP's Zero Day Initiative (ZDI), ICSA-15-153-02 Moxa SoftCMS Buffer Overflow Vulnerability, 6/2/2015.
- Independent researchers Benjamin Kahler and Sebastian Kraemer of HSASec, ICSA-15-148-01 IDS RTU 850 Directory Traversal Vulnerability, 5/28/2015.
- Ivan Sanchez from Nullcode Team, ICSA-15-141-01 Schneider Electric OFS Server Vulnerability, 5/21/2015.
- Security researchers Lucas Apa and Carlos Mario Penagos Hollman of IOActive, ICSA-14-202-01A OleumTech WIO Family Vulnerabilities, 5/21/2015.
- Ivan Sanchez of WiseSecurity Team, ICSA-15-111-02 Rockwell Automation RSLinx Classic Vulnerability, 5/7/2015.

Upcoming Events

July 2015

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

July 27-31

Idaho Falls, Idaho

CLOSED

September 2015

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

Septemter 21-25

Idaho Falls, Idaho

Course Description and Registration

October 2015

Fall 2015 ICSJWG Meeting

October 27-29

Savannah, Georgia

Registration and additional information will be posted here when available:

https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

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 ICS stakeholders. As we develop and prepare new products, we need and want your input. 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/ics-cert/.

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://forms.us-cert.gov/ncsd-feedback/.