Homeland Security

ICS-CERT MONITOR

Contents

National Cybersecurity and Communications Integration Center

Contact Information

For any 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

I Want To:

- Report an ICS incident to ICS-CERT
- Report an ICS software vulnerability
- Get information about reporting

Downloading PGP/GPG Keys
https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT.asc

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. Send your name, telephone contact number, email address, and company affiliation to ics-cert@hq.dhs.gov requesting consideration for portal access.

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/

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

Incident Response Activity

Notable Incident

Water Treatment Facility: Misconfigured Equipment

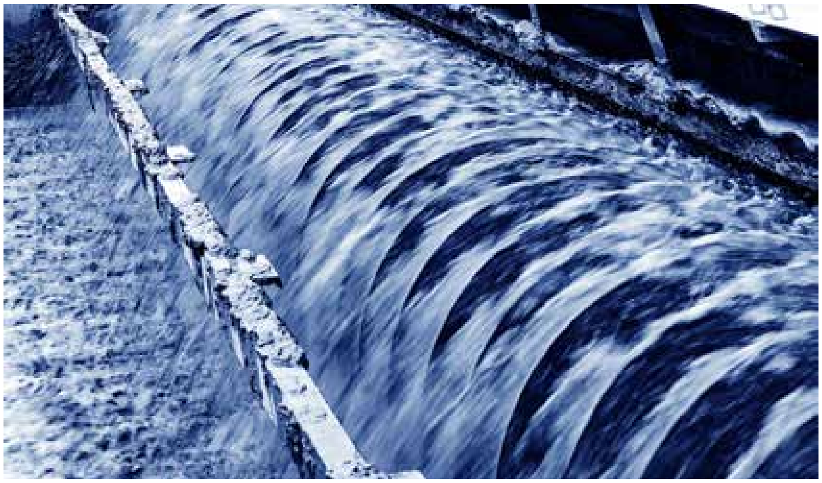
During a recent network infrastructure upgrade, a water utility implemented a misconfigured switch configuration, which flooded the network with traffic. This error led to massive resource consumption on control system endpoints. To the entity, it looked as though the systems had been infected with malware.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) analyzed the router and switch configurations and found an error in how the spanning-tree protocol, which prevents network traffic re-broadcasting loops, was configured. The misconfiguration caused too much network traffic to be sent to endpoint devices, which overloaded the system processors.

ICS-CERT provided its analysis to the utility, which then made corrections to the configurations to correct the spanning-tree errors. All endpoints are now operating correctly.

ICS-CERT has the following recommendations to consider when upgrading infrastructure:

- Engage with the integrators of new systems to ensure compatibility and proper configuration with current systems
- If available, test new configurations in a lab environment to determine what consequences may arise from configuration changes
- Ensure that the integrator is on site when the new configurations are turned on and provide IT staff information and guidance for troubleshooting any issues once the integrator has left.



Onsite Assessments Summary

ICS-CERT Assessment Activity for March/April 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 March/April 2015, ICS-CERT conducted 21 onsite assessments across four sectors (Table 1). Of these 21 assessments, eight were Cyber Security Evaluation Tool (CSET®) assessments, seven were Design Architecture Review (DAR) assessments, and six were Network Architecture Verification and Validation (NAVV) assessments (Table 2).

Assessment Offerings

CSET is a stand-alone software tool that enables users to assess their network and cybersecurity methodology against recognized industry and government standards, guidelines, and best practices.

The DAR assessment provides ICS asset owners with a comprehensive evaluation and discovery process, focusing on defense strategies associated with an asset owner's specific control systems network. The DAR includes an in-depth review and evaluation of the control system's network design, configuration, interdependencies, and its applications.

The NAVV assessment provides a sophisticated analysis of the asset owner's network packet-data. Using a combination of open source and commercially available tools, ICS-CERT passively analyzes the data and develops a detailed representation of the communications flows and relationships between devices.

For more 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 2015.

Assessments by Sector	2015		March/April Totals
	March	April	
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	2		2
Financial Services			
Food and Agriculture			
Government Facilities	2		2
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems	3		3
Water and Wastewater Systems	6	8	14
Monthly Totals	13	8	21 Total Assessments

Table 2. Assessments by type, March/April 2015.

Assessments by Type	2015		March/April Totals
	March	April	
CSET	6	2	8
DAR	4	3	7
NAVV	3	3	6
Monthly Totals	13	8	21 Total Assessments

Situational Awareness

Multi-Factor Authentication

Multi-Factor Authentication Isn't Always What You Think

Authentication is a pillar of information security and, as such, software vendors have chosen several ways to implement it. Seeking to increase user productivity and reduce user frustration, Microsoft implemented a single sign-on feature that allows users to authenticate once and still access multiple separate network services and resources. Unfortunately, this feature also inadvertently introduced a vulnerability that has become a common exploit called "pass-the-hash." *(Microsoft identified this vulnerability and has released information providing holistic planning strategies that, when combined with the Windows security features, provide a more effective defense against pass-the-hash attacks. Go to* www.microsoft.com/pth *for information.)*

Multi-factor authentication is often recommended as a more secure method of authentication. The concept is sound: authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Multi-factor authentication attempts to verify that users are who they claim to be by requiring them to identify themselves with a combination of different authentication factors:

- Something they know, such as a password or personal identification number (PIN)
- Something they have, such as a token or smart card
- Something they are (biometrics), such as a fingerprint

Multi-factor authentication is good for mitigating password-guessing attacks and compromised passwords, but it does not offer protection against all the efforts to subvert a system's authentication mechanisms. Primary among these efforts is the pass-the-hash attack.

Why Multi-Factor Authentication Doesn't Fix Pass-The-Hash

In order to allow users to access network file shares and applications without presenting multiple authentication factors every time, the users' credentials must be stored and presented by the operating system each time a network service needs to authenticate. The Windows operating system uses a stored hash to authenticate a user to a service or resource. Unfortunately, this means that the hash needs to be stored on the system for future reference by the operating system. This storage is what makes the system susceptible to the pass-the-hash attack.

The Windows multi-factor authentication implementation authenticates a user when they log onto the system using something they have (a smart card or key fob) and something they know (a PIN), and then creates an NTLM hash and Kerberos ticket to be stored in memory and used for authentication. This means that Windows takes the multi-factor authentication requirement and reduces it down to the same type and number of tokens that are generated with a simple password login. Therefore, in spite of the security gains against password-guessing attacks, multi-factor authentication does nothing to address the issues that make pass-the-hash so dangerous.

When Multi-Factor Authentication Makes You Less Secure

Not only can smart cards provide a false sense of invincibility, they actually are more susceptible to persistent pass-the-hash attacks. When an account is configured to require smart cards for interactive login, each account has a random value generated by the system that is assigned as the account's password. This value is then stored in the domain controller and retrieved whenever that user logs in with their smart card. However, the system never changes this stored value even if the "password" age is set to expire, unlike when a user is forced to change an expired password in the traditional username/password architecture. This is a perfect scenario for any attacker looking for credentials that have a long shelf life.

This weakness can be overcome if an administrator is knowledgeable enough to implement a script to toggle a particular system setting that forces the computer to regenerate the password for all smart card-enabled accounts, or if they programmatically generate new hashes for all smart card users. Unfortunately, both of these measures will also terminate any active connections being used during the "reset," thereby increasing user frustration and possibly account lock-outs.

Recommendation

With pass-the-hash commonly being employed by attackers, and Windows authentication protocols designed around using hashes for single sign-on, it has become incredibly difficult to track malicious actors once they are legitimized and crawling through the network. With multi-factor authentication unable to address this vulnerability, and with multiple ways of reliably penetrating the perimeter of the environment, defenders need to become more familiar with their networks and what “normal” looks like. Multi-factor authentication does offer some improvements to the outer “shell” of the network, but despite the high-cost of implementing these solutions, they leave the innards of the network still exposed to lateral movement by those they are supposed to stop.

If organizations have evaluated the risks and benefits of using multi-factor authentication on Windows networks and have already implemented or are planning on implementing a multi-factor authentication solution, especially with smart cards, administrators should remember to address the earlier described shortcomings. In particular, administrators should regularly change the static hash by toggling the SmartcardLogonRequired option in Active Directory associated with the user’s account or programmatically generating new passwords through a script or program. It is worth remembering, if users are logged in when their hash is changed, their cached credentials will be invalid and single sign-on authentication will stop working and may even cause an account lockout because of too many authentication failures.

Regardless if multi-factor authentication is used, many layers of defense, including anomaly and signature-based detection methods, are highly recommended for identifying an incident in the early stages. In particular, if incident responders are able to stop an attack before domain accounts with administrative rights (the proverbial keys to the kingdom) are compromised, it is more likely that the attacker can be easily removed from the environment.

ICS-CERT has released guidance on reducing the risk to administrative accounts in ICS-TIP-12-146-01B. Microsoft has released patches for Windows 7 and 8 that help to address some weaknesses in the operating system that are exploited when using pass-the-hash tools. Verifying that systems are up to date and can help to mitigate some of the risk of attack.

More information about pass-the-hash attacks and how to mitigate them can be found here:

- www.microsoft.com/pth
- ”Mitigating Pass-the-Hash and Other Credential Theft, v1,” Microsoft Corporation, 2012
- “Mitigating Pass-the-Hash and Other Credential Theft, v2,” Microsoft Corporation, 2014

ICS-CERT News

ICSJWG Spring Meeting

The next Industrial Control Systems Joint Working Group (ICSJWG) meeting will be held on June 23–24, 2015, at the Wilbur J. Cohen Building, 330 Independence Avenue SW, Washington, D.C. This ICSJWG meeting will bring together asset owners and operators, government professionals, vendors, systems integrators, and academic professionals to discuss the latest initiatives impacting the security of our critical infrastructure. For this meeting, we are shifting priorities toward expanding stakeholder collaboration by providing activities that facilitate inter-sector communication and strengthen role interactions and networking. The meeting will include keynote speakers, practical demonstrations, plenary presentations, panel presentations, and non classified briefings. A classified briefing will be held on June 25 at a separate location (for US citizens only). For important additional information and to register, go to https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

ICS-CERT Regional Training

ICS-CERT continues to offer regional training sessions on cybersecurity for ICSs. This training is provided specifically for the personnel responsible for the oversight, design, and operation of control systems. This includes operators, engineers, IT personnel, supervisors, and managers. Regional training sessions are presented in various locations, multiple times per year.

These sessions offer three courses of escalating difficulty. The Introduction to Industrial Control Systems Cybersecurity (Course 101) is an 8-hour lecture-only course that introduces students to the basics of ICS security. The Intermediate Cybersecurity for Industrial Control Systems (Course 201) is also an 8-hour lecture-only course providing technical instruction on the protection of ICSs using offensive and defensive methods. The final course, Intermediate Cybersecurity for Industrial Control Systems, Part 2 (Course 202) is an 8-hour hands-on course structured to help students understand exactly how attacks against ICS could be launched and why they work. It also provides mitigation strategies to increase the cybersecurity posture of the ICS network. Accompanying networks are used to demonstrate exploits and mitigation tactics in the various exercises. This helps the students develop ICS cybersecurity skills they can apply when they return to their jobs.

The regional training typically runs Monday through Thursday. The 101 and 201 courses are taught Monday and Tuesday and engage up to 100 attendees. The 202 course is taught both on Wednesday and Thursday and is limited to approximately 40 attendees because of the hands on nature of the course. Students are able to register for each course separately, allowing for a customized learning experience. ICS-CERT is sponsoring these sessions, and there are no course fees. Attendees are responsible for all travel, food, and lodging expenses. To register for an ICS-CERT provided training, go to https://ics-cert.us-cert.gov/Calendar.

CSET 6.2

The latest version of ICS-CERT's Cyber Security Evaluation Tool (CSET®), CSET 6.2, was released on January 30, 2015. CSET is a desktop software tool that guides you through a step-by-step process to assess ICSs and information technology (IT) network security practices against recognized industry standards. CSET offers a systematic and repeatable approach and provides a prioritized list of recommendations.

There are many benefits from using the CSET tool. CSET raises awareness and facilitates discussion on cybersecurity within your organization. It highlights vulnerabilities in your organization's systems and provides recommendations on ways to address each vulnerability.

U.S. DEPARTMENT OF HOMELAND SECURITY
CYBER SECURITY EVALUATION TOOL
CSET®

CSET provides a method to systematically compare and monitor improvement in your organization's cyber systems. It identifies areas of strength and best practices being followed in your organization, and it contributes to your organization's risk management and decision-making process. Overall, CSET provides a common industry-wide tool for assessing cyber systems.

What's New in CSET 6.2?

The following new features have been added to the latest version of CSET:

- New Industry Standards
  - North American Electric Reliability Corporation (NERC) CIP-002 through CIP-011, Rev 5
  - Committee on National Security Systems Instruction (CNSSI) No. 1253 Baseline V2 March 27, 2014.
- New Diagramming Capabilities
  - Associate multiple components together by using the new multiple services component. This feature allows the user to more closely model the real world where multiple services are typically added to one machine.
  - Added a diagram inventory that provides the ability to visualize and update all diagram components in a tabular format. All diagram components can also be exported to Excel. This feature brings all diagram components together for easy maintenance and sorting.
  - Added description fields to components, which allows the user to keep notes or other important information concerning diagram components.
  - New component stencils have been added to CSET 6.2, which are also usable in Visio 2013.
- New Import/Export Capabilities
  - Import Visio 2013 diagrams into CSET 6.2. Click the import Visio button on the diagram screen to bring in Visio diagrams.
  - Export CSET 6.2 diagrams to Visio 2013 format. Users can now create a diagram in CSET 6.2, export it, and open it up in Visio 2013.
  - Import diagrams into CSET 6.2 from files generated by the Grassmarlin.
- New Department of Defense (DOD) support
  - New support for National Institute for Standards and Technology (NIST) 800-60 special factors
  - eMass users can import CSET 6.2 data directly into the eMass software.

CSET is distributed freely to the public. For additional information on CSET or to download a copy, go to https://ics-cert.us-cert.gov/assessments. The defect reporting and feature request web site is available at http://cset.inl.gov

Recent Product Releases

Advisories

ICSA-15-120-01 OPTO 22 Multiple Product Vulnerabilities, 4/30/2015.

ICSA-15-064-01A Siemens SIMATIC HMI Basic, SINUMERIK, and Ruggedcom APE GHOST Vulnerability, 4/23/2015.

ICSA-15-064-02A Siemens SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER Insufficiently Qualified Paths, 4/23/2015.

ICSA-15-099-01A Siemens SIMATIC HMI Devices Vulnerabilities, 4/23/2015.

ICSA-15-097-01 Moxa VPort ActiveX SDK Plus Stack-Based Buffer Overflow Vulnerability, 4/7/2015.

ICSA-15-092-01 Schneider Electric VAMPSET Software Buffer Overflow Vulnerability, 4/2/2015.

ICSA-15-090-01 Inductive Automation Ignition Vulnerabilities, 3/31/2015.

ICSA-15-090-02 Ecava IntegraXor DLL Vulnerabilities, 3/31/2015.

ICSA-15-090-03 Hospira MedNet Vulnerabilities, 3/31/2015.

ICSA-15-085-01A Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Vulnerabilities, 3/31/2015.

ICSA-15-036-01A GE and MACTek HART Device DTM Vulnerability, 3/25/2015.

ICSA-15-062-02 Rockwell Automation FactoryTalk DLL Hijacking Vulnerabilities, 3/19/2015.

ICSA-15-076-01 XZERES 442SR Wind Turbine Vulnerability, 3/17/2015.

ICSA-15-076-02 Honeywell XL Web Controller Directory Traversal Vulnerability, 3/17/2015.

ICSA-14-350-02 Johnson Controls Metasys Vulnerabilities, 3/17/2015.

ICSA-15-071-01 Schneider Electric Pelco DS-NVs Buffer Overflow Vulnerability, 3/12/2015.

ICSA-15-069-04A Elipse E3 Process Control Vulnerability, 3/11/2015.

ICSA-15-069-01 Cimon CmnView DLL Hijacking Vulnerability, 3/10/2015.

ICSA-15-069-02 ABB HART Device DTM Vulnerability, 3/10/2015.

ICSA-15-069-03 SCADA Engine BACnet OPC Server Vulnerabilities, 3/10/2015.

ICSA-15-041-02 GE Hydran M2 Predictable TCP Initial Sequence Vulnerability, 3/10/2015.

ICSA-15-064-03 Siemens SPC Controller Series Denial-of-Service Vulnerability, 3/5/2015.

ICSA-15-064-04 Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability, 3/5/2015.

ICSA-15-064-05 Siemens SPCanywhere App Vulnerabilities, 3/5/2015.

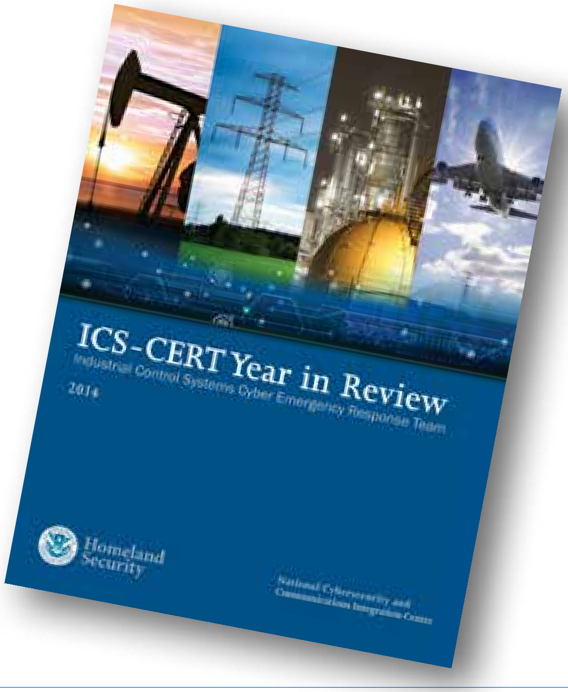
ICSA-14-353-01 Network Time Protocol Vulnerabilities (Supplement Update A), 3/5/2015.

ICSA-15-062-01 MICROSYS PROMOTIC Stack Buffer Overflow, 3/3/2015.

Other

ICS-CERT Monitor September 2014 – February 2015

ICS-CERT Year in Review 2014

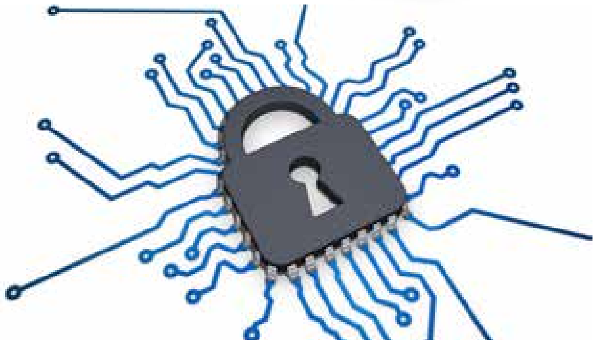

ICS-CERT Year in Review
Industrial Control Systems Cyber Emergency Response Team
2014
Homeland Security
National Cybersecurity and Communications Integration Center

Open Source Situational Awareness Highlights

Leak investigation stalls amid fears of confirming U.S.-Israel operation

2015-03-10

http://www.washingtonpost.com/world/national-security/leak-investigation-stalls-amid-fears-of-confirming-joint-us-israel-operation/2015/03/10/2a348b1e-c36c-11e4-9ec2-b418f57a4a99_story.html



Coordinated Vulnerability Disclosure

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

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at

ics-cert@hq.dhs.gov or toll free at 1-877-776-7585.

Researchers Assisting ICS-CERT with Products Published March–April 2015

ICS-CERT appreciates having worked with the following researchers:

- Ivan Sanchez from Nullcode Team, ICSA-15-120-01 OPTO 22 Multiple Product Vulnerabilities, 4/30/2015.
- Ivan Sanchez from WiseSecurity Team, ICSA-15-064-02A Siemens SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER Insufficiently Qualified Paths, 4/23/2015.
- HP's Zero Day Initiative (ZDI), ICSA-15-097-01 Moxa VPort ActiveX SDK Plus Stack-Based Buffer Overflow Vulnerability, 4/7/2015.
- Evgeny Druzhinin, Alexey Osipov, Ilya Karpov, and Gleb Gritsai of Positive Technologies, ICSA-15-090-01 Inductive Automation Ignition Vulnerabilities, 3/31/2015.
- Security researcher Praveen Darshanam, ICSA-15-090-02 Ecava IntegraXor DLL Vulnerabilities, 3/31/2015.
- Independent researcher Billy Rios, ICSA-15-090-03 Hospira MedNet Vulnerabilities, 3/31/2015.
- Gleb Gritsai, Ilya Karpov, and Kirill Nesterov of Positive Technologies Security Lab and independent researcher Alisa Esage Shevchenko, ICSA-15-085-01A Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Vulnerabilities, 3/31/2015.
- Alexander Bolshev and Svetlana Cherkasova of Digital Security, ICSA-15-036-01A GE and MACTek HART Device DTM Vulnerability, 3/24/2015.
- Ivan Sanchez of NullCode & Evilcode Team, ICSA-15-062-02 Rockwell Automation FactoryTalk DLL Hijacking Vulnerabilities, 3/19/2015.
- Independent researcher Maxim Rupp, ICSA-15-076-01 XZERES 442SR Wind Turbine Vulnerability, 3/17/2015.
- Martin Jartelius of Outpost24, ICSA-15-076-02 Honeywell XL Web Controller Directory Traversal Vulnerability, 3/17/2015.
- Independent security researcher Billy Rios, ICSA-14-350-02 Johnson Controls Metasys Vulnerabilities, 3/17/2015.
- HP's ZDI, ICSA-15-071-01 Schneider Electric Pelco DS-NVs Buffer Overflow Vulnerability, 3/12/2015.
- Ivan Sanchez from Nullcode Team, ICSA-15-069-04A Elipse E3 Process Control Vulnerability, 3/11/2015.
- Ivan Sanchez of Wise Security, ICSA-15-069-01 Cimon CmnView DLL Hijacking Vulnerability, 3/10/2015.
- Alexander Bolshev of Digital Security, ICSA-15-069-02 ABB HART Device DTM Vulnerability, 3/10/2015.
- Independent researcher Josep Pi Rodriguez, ICSA-15-069-03 SCADA Engine BACnet OPC Server Vulnerabilities, 3/10/2015.
- 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-15-041-02 GE Hydran M2 Predictable TCP Initial Sequence Vulnerability, 3/10/2015.
- Davide Peruzzi of GoSecure!, ICSA-15-064-03 Siemens SPC Controller Series Denial-of-Service Vulnerability, 3/5/2015.
- Johannes Klick, Christian Pfahl, Martin Gebert, and Lucas Jacob from Freie Universität Berlin's work team SCADACS, ICSA-15-064-04 Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability, 3/5/2015.
- Karsten Sohr, Bernhard Berger, and Kai Hillmann from the TZI-Bremen, Kim Schlyter, Seyton Bradford, and Richard Warren from FortConsult, and Stefan Schuhmann, ICSA-15-064-05 Siemens SPCanywhere App Vulnerabilities, 3/5/2015.
- An anonymous researcher working with HP's Zero Day Initiative, ICSA-15-062-01 MICROSYS PROMOTIC Stack Buffer Overflow, 3/3/2015.

Follow ICS-CERT on Twitter: @icscert

Upcoming Events

June 2015

Regional Cybersecurity Training for Industrial Control Systems (3 days)

June 1–4, 2015

Salt Lake City, Utah

CLOSED

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

June 15–19

Idaho Falls, Idaho

CLOSED

ICSJWG 2015 Spring Meeting

June 23–24

Washington, DC

[Information and Registration]

July 2015

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

July 13-17

Idaho Falls, Idaho

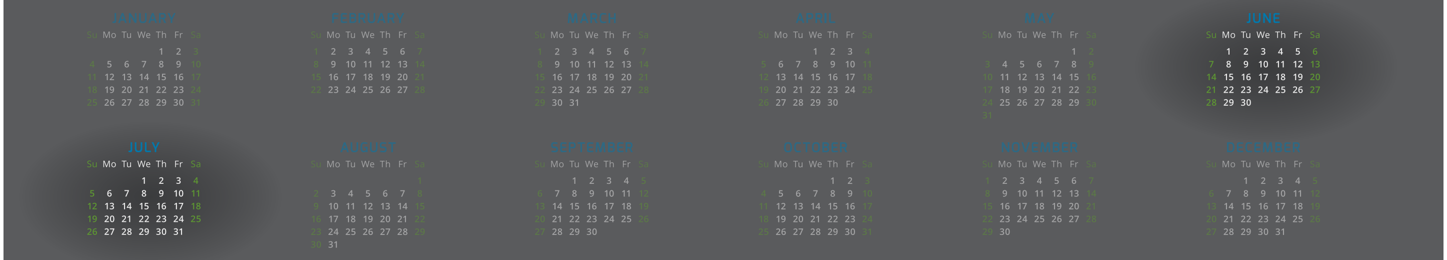
CLOSED

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

July 27-31

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.

Document FAQ

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

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