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

Incident Response Activity

Notable Incident

In July, ICS-CERT became aware of a spear-phishing campaign by advanced persistent threat (APT) actors that targeted multiple sectors, including Chemical, Critical Manufacturing, Energy, and Government Facilities. The activity involved emails with links that redirected to web sites hosting malicious files that exploited a zero-day vulnerability (since then patched) in Adobe Flash Player (CVE-2015-3113).

In previous incidents occurring in early 2014, the same actors also used various social engineering tactics and social media to perform reconnaissance and target company employees. In one case, the malicious actors used a social media account to pose as a perspective candidate for employment and opened a dialogue with employees of a critical infrastructure asset owner. The actors asked probing questions such as the name of the company's IT manager and versions of the current running software. The actor subsequently requested feedback on a resume and sent a "resume.rar" archive email attachment for review to the employee's personal email account. The resume.rar archive contained three files including a malicious version of the open-source TTCalc application that infected the employee's computer with Backdoor.APT.CookieCutter. ICS-CERT worked with the affected entity to confirm that the incident occurred on their business network and was quickly contained. No control systems were impacted.

The use of social media and zero-day exploits illustrates a concerted effort to gain access to critical infrastructure networks

While the motivations of the APT actors remain unknown, the use of social media and zero-day exploits illustrates a concerted effort to gain access to critical infrastructure networks. In response, ICS-CERT published an alert (ICS-ALERT-15-198-01P APT Spearphishing Campaign Against Multiple Sectors) to the secure portal to consolidate previous campaign indicators with new indicators for network defenders to use. This Alert is available to asset owners/operators who have portal accounts in the Control Systems Center on the US-CERT secure portal (https://portal.us-cert.gov). Asset owners/operators can request a portal account by sending an email to ics-cert@hq.dhs.gov.

As with any malicious and targeted cyber activity, ICS-CERT requests feedback and reporting if your organization has been targeted by this or similar activity. Reporting your cyber events and incidents to ICS-CERT helps the community at large have a better understanding of the activity occurring across sectors and the techniques/indicators of compromise (IOCs) being used. ICS-CERT will protect and anonymize your information and only share the technically relevant information (such as IOCs) with partners that have a need to know.

Onsite Assessments Summary

ICS-CERT Assessment Activity for July/August 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 July/August 2015, ICS-CERT conducted 22 onsite assessments across five sectors (Table 1). Of these 22 assessments, two were Cyber Security Evaluation Tool (CSET®) assessments, 14 were Design Architecture Review (DAR) assessments, and six were Network Architecture Verification and Validation (NAVV) assessments (Table 2). The 10 assessments performed for the Emergency Services sector were DARs that included analyzing a variety of building and facility management systems (e.g., Power Distribution and Transmission, HVAC, lighting, perimeter protection, access control, and fire suppressions systems) utilized in support of continuity of operations facilities and sites. For detailed information on ICS-CERT's CSET, DAR, and NAVV assessments, go to https://ics-cert.us-cert.gov/assessments.

Table 1: Assessments by sector, July/August 2015.

Assessments by Sector	July 2015	August 2015	July/August Totals
Chemical		3	3
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services	10		10
Energy	3		3
Financial Services			
Food and Agriculture			
Government Facilities		4	4
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems	2		2
Monthly Totals	15	7	22 Total Assessments

Table 2. Assessments by type, July/August 2015.

Assessments by Type	July 2015	August 2015	July/August Totals
CSET	1	1	2
DAR	10	4	14
NAVV	4	2	6
Monthly Totals	15	7	22 Total Assessments

Situational Awareness

Logging

The digital world is expanding at a massive rate, and along with new advancements comes new software and increasingly complex systems. As more software comes together and interacts to implement new features, applications grow in complexity and scale. Developers use a variety of techniques to keep track of what is going on behind the scenes. Logging is one of the more common techniques used.

Logs can be thought of as receipts for the actions that an application performs. These receipts are generated either by the application itself, by the database to which it connects, or by the operating system on which the application is running. The level of detail on each receipt is determined by the software that issued it.

Logging is frequently used in software development to keep track of when specific operations happen. Developers, troubleshooters, and analysts use logs to investigate the operations performed by an application surrounding some particular event, as well as to monitor for how a system is performing. A system owner could use recorded logging to find issues within a system (for example, why information from a connected device is not populating a monitoring application).

Suppose that a temperature sensor frequently collected temperatures that suddenly spike up or down unexpectedly. Creating logs of the information transmitted by the device gives the owner the information to determine what is happening when the temperature spikes occur. The work of determining where an error is coming from can be reduced dramatically by regular review and analysis, potentially reducing time taken to repair an issue from days down to minutes. The owner will need less time for troubleshooting and can potentially avoid the loss of any hardware mistakenly assumed to be faulty.

The first step in leveraging a system's logging is understanding what capabilities are available. Some systems provide excellent levels of logging that are configurable; others may provide nothing at all. In the latter case, users are forced to creatively employ third-party solutions. Otherwise, the biggest challenge will be determining the proper level of logging that an application is generating by balancing between memory consumed, history of events, and how much data are kept with each log entry. Google details this tradeoff at: (http://googletesting.blogspot.com/2013/06/optimal-logging.html). Too much information becomes noise and can take up a great deal of space, and too little could pose issues when pinning down the problems or anomalies that logging was developed to find.

A detailed history of events that have occurred on a system can be an essential asset, especially when the system is supporting any critical or sensitive information. Records of accessed information, communications made between servers, and actions performed by users can be vital for damage assessment after a breach, as well as in detecting breaches when they have occurred. By regular review of system and database logs, administrators will become familiar with what usage patterns they expect to see on their systems and, in turn, what usage patterns seem unusual, even if automated security tools have missed something or been bypassed.

In critical applications and security systems that require a great deal of oversight, logs must preserve a large amount of transaction history, potentially stretching all the way back until the system was first activated. For other applications, logging past the current day may not be helpful. What information is preserved and for how long is reliant on the criticality of the system and may be challenging for the administrator to determine. The National Institute of Standards and Technology (NIST) offers guidance on determining the level of logging needed to satisfy the lawful requirements in a number of business cases and general recommendations for a variety of other fields not specifically addressed (http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf).

The most important thing to keep in mind with logging and log files in general is that they provide a history of the system that needs to be reviewed. If integrated into the normal operating procedures, logging can quickly provide key insight into increasingly complex systems. Whether it is an engineer or technician troubleshooting a problem or a security investigator looking for potential concerns, this history can offer insights that can keep an organization from becoming front page news.

ICS-CERT NEWS

ICS-CERT International

The role of ICS-CERT is to protect our 16 critical infrastructure sectors, laid out in Presidential Policy Directive 21, from cyber-originating harm. The risks to industrial control systems are not geographically limited; in an interconnected world, cyber risk is global by default. In particular, recent malware campaigns demonstrate that control systems directly facing the Internet get compromised without properly implemented security measures. In addition, supply chain, manufacturing, and markets are all global endeavors. Therefore, a discovered vulnerability in one product may be exploitable in systems around the world. The ubiquitous nature of industrial control systems products means that nefarious actors looking to discover vulnerabilities are more able to analyze products and systems. In many cases, the ability to obtain and study a system is key to exploiting it. Even if a cyber-event doesn't touch U.S. critical infrastructure, the same tactics may be used against the United States at a later date. In this interconnective environment, international engagement is both a strategic necessity and an operational imperative for the Department of Homeland Security's (DHS) cybersecurity mission.

In the United States, critical infrastructure is held primarily by the private sector. In some cases, federal, state, or municipal governments may own part of an asset, but approximately 85 percent of our critical infrastructure is owned, operated, and controlled by the private sector. This private sector dynamic is not necessarily present in partner countries where a government may play a more forward role in critical infrastructure. Within each country, the responsibility for industrial control systems is handled differently with regard to both scope and organization. The responsibility may be broken out over multiple agencies with each being responsible for different sectors, or a country may choose to define its critical infrastructure to encompass completely different areas of national infrastructure and the economy. The different setup in each country means that when ICS-CERT interacts with international counterparts it is often with a variety of different organizations rather than just the "ICS-CERT" for that country.

In the international community, cyber is playing an ever increasing role, and global organizations have recognized the need to address cyber issues. However, the responsibility for securing systems remains on states and the private entities who own the networks. Industrial control systems particularly are just beginning to be explored both from a strategic and tactical perspective. For example, this year ICS-CERT participated in the International Atomic Energy Association's (IAEA) first computer security conference to deal with issues of security specifically in nuclear systems. The nuclear sector is highly regulated worldwide with comprehensive oversight, but a robust, ongoing discussion of cybersecurity is still emerging, rather than ad hoc conversation in response to specific issues.

In addition, in 2015 ICS-CERT also attended the Annual Forum of Incident Response and Security Teams (FIRST) in Berlin, Germany. FIRST is a global non-profit organization dedicated to bringing together cyber emergency response team from across the globe, including response teams from over 300 member teams from over 60 countries representing government agencies, academia, commercial enterprises, and financial corporations. FIRST is unique in that it is one of the only international events where representatives from ICS-CERT can network, collaborate, and build relationships with its international operational peers from the public and private sectors.

Within the DHS National Protection and Programs Directorate (NPPD), the Office of Cybersecurity and Communications (CS&C) International Affairs Program serves as the focal point for coordinating international efforts in support of DHS's cybersecurity and communications mission. This includes supporting the National Cybersecurity and Communications Integration Center (NCCIC) in fostering cooperation with and among global stakeholders to address cybersecurity risks. Much of ICS-CERT's coordination on international engagements is done in tandem with US-CERT to benefit from its pre-existing relationships with other CERTs. ICS-CERT's engagement with the international community covers a wide range of activities from meetings and speaking engagements to product development and mutual participation in the Industrial Control Systems Joint Working Group (ICSJWG). ICS-CERT also works with the international community to share information. By engaging with the international community to foster operational collaboration and share information, we improve our collective situational awareness and response to current threats.

If you, or your organization, are interested in learning more about ICS-CERT's international efforts, please contact us at ICS-CERTInternational@hq.dhs.gov.

CSET 7.0

ICS-CERT released the latest version of its Cyber Security Evaluation Tool (CSET), CSET 7.0, in early August 2015. CSET provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. It is a desktop software tool that guides asset owners and operators through a step-by-step process to analyze their ICS and IT network security practices using many recognized government and industry standards and recommendations.

The process is simple. Select a standard and security assurance level (SAL), import or create a network diagram, then answer a series of questions about system components and architecture, as well as operational policies and procedures. CSET compares the responses to the relevant security standards, assesses overall compliance, and provides appropriate recommendations for improving the system's cybersecurity posture. The interactive dashboard and customizable reports feature multiple charts, including standards compliance, top areas of concern, and prioritized controls that are based on real cybersecurity incident information. CSET also supports the ability to compare multiple assessments, establish a baseline, and determine trends.

What's New?

- Additional standards were included:
  - Cybersecurity Capability Maturity Model (C2M2), Version 1.1.
  - Department of Defense (DoD) Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT).
  - National Institute of Standards and Technology Interagency Report (NISTIR) 7628 Volume 1, Revision 1, Guidelines for Smart Grid Cybersecurity.
- The user interface was completely redesigned with a new, more modern look and intuitive interface. Additional landing pages were added at each major step in the process that contain instructions to help the user understand the purpose of the associated sections.
- Improved the functionality of the Questions screen:
  - Increased the responsiveness when answering questions and filtering.
  - Added the ability to change the Question text size for improved readability.
  - Updated the Supplemental Information section for questions related to the C2M2, NRC, COR 7, and Key standards.
- Added the ability to encrypt assessment files within CSET.

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. To report a problem or request a new feature, go to http://cset.inl.gov.

Medical Device Cybersecurity

ICS-CERT might not be the first organization that comes to mind when thinking of medical device cybersecurity. However, Healthcare and Public Health is one of the 16 critical infrastructure sectors defined by Presidential Policy Directive 21, and our work with medical device vendors on software and hardware vulnerability coordination has been increasing over the last 3 years.

Similarities in the underlying embedded hardware and software technologies connect medical device and control system vulnerability exploitation. Programmable logic controllers communicate on a network, have embedded control of processes, and provide human-readable feedback just as, for example, an infusion pump or an MRI does. Vulnerabilities found in a control system device can affect a medical device when standard code libraries are used to develop the embedded operating systems.

ICS-CERT collaborates with the Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), and the National Health Information Sharing and Analysis Center (NH-ISAC). These information sharing relationships are concerned with patient safety rather than regulatory issues and are similar to our relationships with the well-known ES-ISAC (electricity sector) and Water-ISAC (Water and Wastewater Services Sector). Our goal is to provide the same assessment, vulnerability coordination, and incident response services to medical asset owners and operators, as well as device vendors, as we do for those in each of the other 15 critical infrastructure sectors.

ICSJWG Fall 2015 Meeting

The Industrial Control Systems Joint Working Group (ICSJWG) 2015 Fall Meeting will take place at the Coastal Georgia Center in downtown Savannah, GA, on October 27-29. The Meeting will include two and a half days of interactions and discussions through keynote speakers, practical demonstrations, presentations, panels, lightning round talks, and nonclassified briefings. We will also be exploring new sessions in which the membership has shown interest. Some of these anticipated highlights include:

- ICSJWG's first ever Vendor Expo!
- "Ask Me Anything" session with representatives from NCCIC/ICS-CERT
- Break-out/networking session exclusively for our international partners.

The Meeting provides an opportunity for government professionals (federal, state, local, tribal, and international), control systems vendors and systems integrators, research and development and academic professionals, and asset-owners and operators to network with cybersecurity peers and stay abreast of the latest initiatives impacting security for industrial control systems and our critical infrastructure.

For more information, including registration, please visit our web site: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

Recent Product Releases

Alerts

ICS-ALERT-15-225-01A Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability, 8/20/2015.

ICS-ALERT-15-225-02A Rockwell Automation 1766-L32 Series Vulnerability, 8/20/2015.

ICS-ALERT-15-224-01 KAKO HMI Hard-coded Password, 8/12/2015.

ICS-ALERT-15-224-02 Schneider Electric Modicon M340 PLC Station P34 Module Vulnerabilities, 8/12/2015.

ICS-ALERT-15-224-03 Prisma Web Vulnerabilities, 8/12/2015.

ICS-ALERT-15-224-04 Moxa ioLogik E2210 Vulnerabilities, 8/12/2015.

ICS-ALERT-15-203-01 FCA Uconnect Vulnerability, 7/22/2015.

Advisories

ICSA-15-239-01 Moxa SoftCMS Buffer Overflow Vulnerabilities, 8/27/2015.

ICSA-15-239-02 Siemens SIMATIC S7-1200 CSRF Vulnerability, 8/27/2015.

ICSA-15-239-03 Innominate mGuard VPN Vulnerability, 8/27/2015.

ICSA-15-050-01A Siemens SIMATIC STEP 7 TIA Portal Vulnerabilities, 8/27/2015.

ICSA-15-099-01C Siemens SIMATIC HMI Devices Vulnerabilities, 8/27/2015.

ICSA-15-237-01 Endress+Hauser HART Device DTM Vulnerability, 8/25/2015.

ICSA-15-225-01 OSIsoft PI Data Archive Server Vulnerabilities, 8/13/2015.

ICSA-15-223-01 Schneider Electric IMT25 DTM Vulnerability, 8/11/2015.

ICSA-15-211-01 Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Password Storage Vulnerability, 7/30/2015.

ICSA-15-202-01 Siemens SIPROTEC Denial-of-Service Vulnerability, 7/21/2015.

ICSA-15-202-02 Siemens Sm@rtClient Password Storage Vulnerability, 7/21/2015.

ICSA-15-202-03A Siemens RuggedCom ROS and ROX-based Devices TLS POODLE Vulnerability, 7/27/2015.

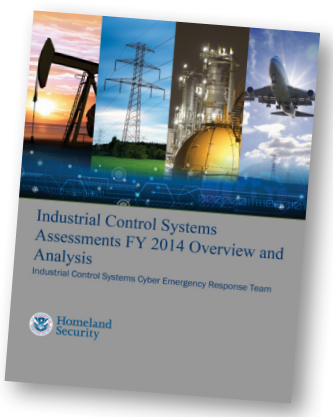
ICSA-15-174-01 Hospira Symbiq Infusion System Vulnerability, 7/21/2015.

ICSA-15-006-01 Eaton's Cooper Power Series Form 6 Control and Idea/IdeaPlus Relays with Ethernet Vulnerability, 7/16/2015.

ICSA-15-195-01 Siemens SICAM MIC Authentication Bypass Vulnerability, 7/14/2015.

Other

Industrial Control Systems Assessments FY 2014 Overview and Analysis, 8/11/2015.

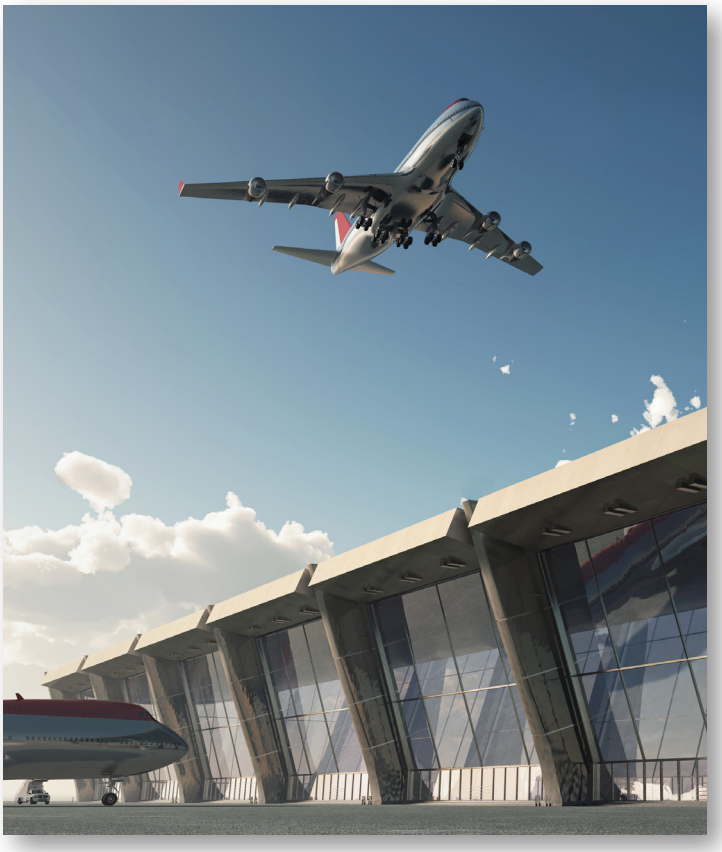


Open Source Situational Awareness Highlights

FAA Convenes Panel to Thwart Airline Cyberattacks

2015-06-29

http://thehill.com/policy/cybersecurity/246415-faa-convenes-panel-to-thwart-airline-cyberattacks



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 July/August 2015

ICS-CERT appreciates having worked with the following researchers:

Alerts

- Aditya K. Sood, ICS-ALERT-15-225-01A Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability (Update A), 8/20/2015.
- Aditya K. Sood, ICS-ALERT-15-225-02A Rockwell Automation 1766-L32 Series Vulnerability (Update A), 8/20/2015.
- Aditya K. Sood, ICS-ALERT-15-224-01 KAKO HMI Hard-coded Password, 8/12/2015.
- Aditya K. Sood, ICS-ALERT-15-224-02 Schneider Electric Modicon M340 PLC Station P34 Module Vulnerabilities, 8/12/2015.
- Aditya K. Sood, ICS-ALERT-15-224-03 Prisma Web Vulnerabilities, 8/12/2015.
- Aditya K. Sood, ICS-ALERT-15-224-04 Moxa ioLogik E2210 Vulnerabilities, 8/12/2015.

Advisories

- HP's Zero Day Initiative, ICSA-15-239-01 Moxa Softcms Buffer Overflow Vulnerabilities, 8/27/2015.
- Alexander Bolshev and Svetlana Cherkasova of Digital Security, ICSA-15-237-01 Endress+Hauser HART Device DTM Vulnerability, 8/25/2015.
- Alexander Bolshev, Gleb Cherbov, and Svetlana Cherkasova of Digital Security, ICSA-15-223-01 Schneider Electric IMT25 DTM Vulnerability, 8/11/2015.
- Gleb Gritsai, Alisa Esage Shevchenko, Ilya Karpov, and the team from Positive Technologies Security, ICSA-15-211-01 Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Password Storage Vulnerability, 7/30/2015.
- Independent researcher Billy Rios, ICSA-15-174-01 Hospira Symbiq Infusion System Vulnerability, 7/21/2015.
- Dr. 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 (NEETRAC), ICSA-15-006-01 Eaton's Cooper Power Series Form 6 Control and Idea/IdeaPlus Relays with Ethernet Vulnerability, 7/16/2015.

Follow ICS-CERT on Twitter: @icscert

Upcoming Events

October 2015

Fall 2015 ICSJWG Meeting

October 27-29

Savannah, Georgia

Description and Registration

November 2015

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

November 16-20

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.