NCCIC

ICS-CERT MONITOR

Contents

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 at the following URL: 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

GovDelivery

ICS-CERT launched a new digital subscription system with GovDelivery to help you stay informed. By signing up for GovDelivery, you can receive new ICS-CERT product release notices directly to your inbox. Learn more, and sign up for GovDelivery at the following URL: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

Downloading PGP/GPG Keys

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

ICS-CERT Services

ICS-CERT Assessments

In this issue of the Monitor, we highlight ICS-CERT Assessments

As a core part of its mission to reduce risk to the Nation's critical infrastructure (CI), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides onsite and remote cybersecurity assessments to CI asset owners and operators to strengthen the cybersecurity posture of their industrial control systems (ICSs). ICS-CERT bases its assessments on standards, guidelines, and best practices and provides them to CI asset owners and operators at no cost using our Congressional funding. The assessment methodology provides a structured framework that asset owners and operators can use to assess, re-assess, protect, detect, and continually validate the cybersecurity of their ICS networks. The information gained from assessments also provides stakeholders with the understanding and context necessary to build effective defense-in-depth processes for enhancing their cybersecurity posture.

ICS-CERT's private sector assessment team works with asset owners to determine which set of assessment services best fits the needs of that particular organization. The services provided may include a combination of a facilitated Cyber Security Evaluation Tool (CSET®), Design Architecture Review (DAR), and/or Network Architecture Verification and Validation (NAVV) assessment, depending on the current state and goals of the organization. The private sector assessment team is transitioning the services it provides from individual CSET, DAR, and NAVV assessments to an integrated process including all the assessment offerings along with more advanced analytics to provide improved actionable feedback to asset owners. The assessment process includes a baseline assessment using CSET, a deep-dive design architecture review of the ICSs, communications, and networking architecture, and analysis of the network data communications.

You can find more information on the ICS-CERT Assessments web page.

Situational Awareness

Preventing DLL Hijacking

Overview

ICS-CERT receives many vulnerability reports regarding Uncontrolled Search Path Elements (CWE-427: https://cwe.mitre.org/data/definitions/427.html), or, more specifically, Dynamic-Link Library (DLL) Hijacking scenarios.

A DLL is a Microsoft "module that contains functions and data that can be used by another module" (https://msdn.microsoft.com/en-us/library/windows/desktop/ms682589(v=vs.85).aspx). DLLs enable modularity within applications for code sharing, reuse, and updates.

DLLs are integral to the Windows architecture but can provide an attack vector if not implemented securely. When a fully qualified path name is not specified, an Uncontrolled Search Path Element (CWE-427) vulnerability can be exploited.

In this scenario, an attacker with local access could rename a malicious DLL to meet the application's search criteria. The application would then be unable to verify that the DLL is correct, allowing the malicious DLL to load. Once loaded, the DLL could run malicious code at the privilege level of the application.

Mitigation

Fortunately, there are mitigation techniques available for this scenario. Microsoft has published guidelines for loading external libraries securely. These can be found on Microsoft's web site: https://msdn.microsoft.com/library/ff919712.

ICS-CERT recommends that developers use these techniques to load external libraries securely whenever possible to avoid Uncontrolled Search Path Element (CWE-427) vulnerabilities and DLL Hijacking scenarios.

HSIN TIP

The Homeland Security Information Network

Now that the Department of Homeland Security (DHS) has consolidated all secure portal capabilities into the Homeland Security Information Network (HSIN), the Monitor will offer tips on how to use the service. HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information with streamlined collaboration and real-time communications throughout all homeland security mission areas. Federal, state, local, territorial, tribal, international, and private sector homeland security partners can use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs. For more information on the HSIN program, please visit the HSIN page on the DHS web site.

Alerts

HSIN provides a simple method that users can employ to be automatically notified whenever the content of a library changes or whenever a specific document within a library changes.

Users can configure their HSIN account to send various types of alerts (all changes, new item posted, etc.), and for various reasons (any change, etc.).

Users can also request immediate notification, a daily summary, or a weekly summary.

HSIN Training provides a brief training course on creating Alerts.

Library Alert

To be notified of changes in a HSIN library,

- Navigate to the library
- Once in the library, on the menu bar click "Library," then click the "Alert Me" icon and choose "Set alert on this library";
- Enter the information in the Alert dialog screen and click "OK" to create the alert (Users may choose to create multiple alerts on a library); and
- Monitor user email for a confirmation message from HSIN.

Document Alert

To be notified of changes to a specific document in a HSIN library,

- Navigate to the library;
- Mouse over the desired document and check the selection box at the left (The box only appears when mousing over it; only check one document at a time);
- Once in the library, on the menu bar click "Documents," then click the "Alert Me" icon and choose "Set alert on this document";
- Enter the information in the Alert dialog screen and click "OK" to create the alert; and
- Monitor user email for a confirmation message from HSIN.

HSIN Training provides a brief training course on creating Alerts.

ICSJWG Spring 2017 Meeting

ICS-CERT is excited to announce that the 2017 Spring Industrial Control Systems Joint Working Group (ICSJWG) Meeting will take place in Minneapolis, Minnesota, at the Loews Minneapolis Hotel. The Spring 2017 meeting will provide a forum for all control systems stakeholders to gather and exchange ideas about critical issues in ICS cybersecurity. This meeting will foster an opportunity for stakeholders to interface with peers, network with industry leaders, and stay abreast of the latest initiatives impacting security for industrial control systems and our critical infrastructure. The spring meeting will include three full days of interactions and discussions in the form of keynote speakers, practical demonstrations, presentations, and panels. The Vendor Expo will return, as will the popular "Ask Me Anything" session by ICS-CERT leadership. For event and registration information, visit the ICSJWG web page. We look forward to seeing you in Minneapolis!

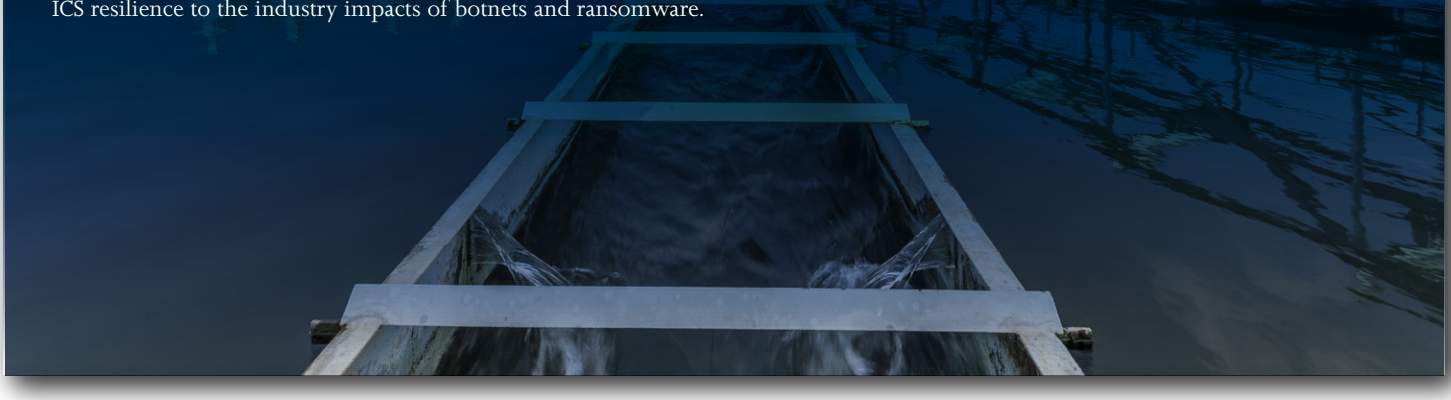
ICS-CERT at S4x17

In January, ICS-CERT attended Digital Bond's S4x17 ICS Security Conference in Miami. This year, S4x17 featured three tracks, including a main stage, a technical "deep dive" stage, and a sponsor stage. Keynote speakers included Mary B. McCord, Acting Assistant Attorney General for National Security at the U.S. Department of Justice, and MedSec Chief Executive Officer Justine Bone.

The main stage highlighted big name speakers and high-level content for the ICS Plant Manager or Chief Information Officer. Among the topics discussed were "the new age of automation," advantages and disadvantages of ICS certification, and coverage of the December 2016 Ukrainian power grid hack. Stage 2 hosted in-depth technical content, such as Schneider Electric's proposed Secure Modbus protocol, deep packet inspection for ICS protocols, and practical attack tools for Analog-to-Digital converters (ADCs). Finally, the sponsor stage featured short but informative talks by S4 sponsors covering a range of ICS-related topics, from ICS resilience to the industry impacts of botnets and ransomware.

Of particular note was the topic of the changing landscape of medical device vulnerability disclosure. Bone's Q&A with Digital Bond's Dale Peterson shed light on the company's decision to pursue uncoordinated disclosure of medical device vulnerabilities, while Joshua Corman, Director of the Cyber Statecraft Initiative of the Atlantic Council, encouraged researchers to continue on the path of coordinated disclosure. Corman emphasized that a trusting relationship based on empathy, in which researchers are perceived as helping hands, is pivotal to positive change.

With a variety of industry professionals in attendance, S4 provided wonderful opportunity for ICS-CERT to meet researchers, develop new industry contacts, and monitor unanticipated vulnerability disclosures. ICS-CERT leverages these opportunities to further its mission of reducing risks to our Nation's critical infrastructure.



Assessments Q&A

Does ICS-CERT connect to our network during an assessment?

The CSET, DAR, and NAVV assessments are all completely hands off; we will not connect to your networks. The only information we will have access to is the information you provide us, such as network diagrams, network header data (for the NAVV assessment), and inventory lists, which we will evaluate prior to visiting with you at your facility. These documents are necessary to schedule and successfully complete your assessment.

Does ICS-CERT do penetration testing?

No. All of our assessment work is performed as a table-top discussion. If you are interested in penetration testing, please contact the National Cybersecurity Assessment & Technical Services (NCATS) program at NCATS@hq.dhs.gov. Select the NCATS Factsheet link for more information.

For more information, see ICS-CERT's Assessment FAQs and Fact Sheet.

PCII Q&A

What is the definition of Critical Infrastructure Information (CII)?

CII is information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, or other information concerning

- Actual, potential, or threatened interference with, attack on, compromise or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct that violates Federal, state, local, or tribal law, harms interstate commerce of the United States, or threatens public health or safety;
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

For further information on CII, please see the Critical Infrastructure Information Act of 2002 (CII Act) and "Procedures for Handling Infrastructure Information; Final Rule" (6 CFR Part 29) available at www.dhs.gov/pcii. For additional questions and answers, see the PCII FAQs.

ICS-CERT Assessment Activity for January/February 2017

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 January/February 2017, ICS-CERT conducted 25 onsite assessments across three sectors (Table 1). Of these 25 assessments, nine were Cyber Security Evaluation Tool (CSET®) assessments, eight were Design Architecture Review (DAR) assessments, and eight 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, January/February 2017.

Assessments by Sector	January 2017	February 2017	January/February Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	7		7
Financial Services			
Food and Agriculture		3	3
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems	12	3	15
Monthly Totals	19	6	25 Total Assessments

Table 2. Assessments by type, January/February 2017.

Assessments by Type	January 2017	February 2017	January/February Totals
CSET	7	2	9
DAR	6	2	8
NAVV	6	2	8
Monthly Totals	19	6	25 Total Assessments

Recent Product Releases

Advisories

ICSA-17-059-01 Siemens RUGGEDCOM NMS, February 28, 2017

ICSA-16-103-03A Siemens Industrial Products DROWN Vulnerability (Update A), February 28, 2017

ICSA-17-054-01 VIPA Controls WinPLC7, February 23, 2017

ICSA-17-054-02 Red Lion Controls Sixnet-Managed Industrial Switches, AutomationDirect STRIDE-Managed Ethernet Switches Vulnerability, February 23, 2017

ICSA-17-054-03 Schneider Electric Modicon M340 PLC, February 23, 2017

ICSA-17-045-01 Advantech WebAccess, February 14, 2017

ICSA-15-342-01C XZERES 442SR Wind Turbine Cross-site Scripting Vulnerability (Update C), February 21, 2017

ICSA-17-045-01 Advantech WebAccess, February 14, 2017

ICSA-17-045-02 Geutebrück IP Cameras, February 14, 2017

ICSA-17-045-03 Siemens SIMATIC Authentication Bypass, February 14, 2017

ICSA-16-343-05A Rockwell Automation Logix5000 Programmable Automation Controller Buffer Overflow Vulnerability (Update A), February 14, 2017

ICSA-17-040-01 Hanwha Techwin Smart Security Manager, February 9, 2017

ICSA-17-038-01 Sielco Sistemi Winlog SCADA Software, February 7, 2017

ICSA-17-031-01A BINOM3 Electric Power Quality Meter (Update A), February 7, 2017

ICSMA-17-017-01 BD Alaris 8000 Insufficiently Protected Credentials Vulnerability, February 7, 2017

ICSMA-17-017-02 BD Alaris 8015 Insufficiently Protected Credentials Vulnerabilities, February 7, 2017

ICSMA-17-009-01A St. Jude Merlin@home Transmitter Vulnerability (Update A), February 6, 2017

ICSA-17-033-01 Honeywell XL Web II Controller Vulnerabilities, February 2, 2017

ICSA-17-031-02 Ecava IntegraXor, January 31, 2017

ICSA-17-026-01 Eaton ePDU Path Traversal Vulnerability, January 26, 2017

ICSA-17-026-02 Belden Hirschmann GECKO, January 26, 2017

ICSA-17-024-01 Schneider Electric Wonderware Historian, January 24, 2017

ICSA-16-336-05A GE Proficy HMI/SCADA iFIX, Proficy HMI/SCADA CIMPLICITY, and Proficy Historian Vulnerability (Update A), January 24, 2017

ICSA-17-019-01 Schneider Electric homeLYnk Controller, January 19, 2017

ICSA-17-017-01 Phoenix Contact mGuard, January 17, 2017

ICSA-17-012-01 Advantech WebAccess, January 12, 2017

ICSA-17-012-02 VideoInsight Web Client, January 12, 2017

ICSA-17-012-03 Carlo Gavazzi VMU-C EM and VMU-C PV, January 12, 2017

ICSA-17-010-01 OSIsoft PI Coresight and PI Web API, January 10, 2017

ICSA-16-336-06 Rockwell Automation MicroLogix 1100 and 1400 Vulnerabilities, January 5, 2017

Follow ICS-CERT on Twitter: @icscert

Open Source Situational Awareness Highlights

Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure

2017-01-06

https://ics-cert.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf

Managing Medical Device Cybersecurity in the Postmarket: At the Crossroads of Cyber-safety and Advancing Technology

2017-01-04

http://blogs.fda.gov/fdavoice/index.php/2016/12/managing-medical-device-cybersecurity-in-the-postmarket-at-the-crossroads-of-cyber-safety-and-advancing-technology/

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 January/February 2017

ICS-CERT appreciates having worked with the following researchers:

- Ariele Caltabiano (kimiya) working with Trend Micro's Zero Day Initiative, ICSA-17-054-01 VIPA Controls WinPLC7, February 23, 2017
- Mark Cross of RIoT Solutions, ICSA-17-054-02 Red Lion Controls Sixnet-Managed Industrial Switches, AutomationDirect STRIDE-Managed Ethernet Switches Vulnerability, February 23, 2017
- Luis Francisco Martin Liras, ICSA-17-054-03 Schneider Electric Modicon M340 PLC, February 23, 2017
- Karn Ganeshen and Tim Thurlings, ICSA-15-342-01C XZERES 442SR Wind Turbine Cross-site Scripting Vulnerability (Update C), February 21, 2017
- Li MingZheng Kuangn, ICSA-17-045-01 Advantech WebAccess, February 14, 2017
- Florent Montel and Frédéric Cikala, ICSA-17-045-02 Geutebrück IP Cameras, February 14, 2017
- Steven Seeley of Source Incite, ICSA-17-040-01 Hanwha Techwin Smart Security Manager, February 9, 2017
- Karn Ganeshen, ICSA-17-038-01 Sielco Sistemi Winlog SCADA Software, February 7, 2017
- Karn Ganeshen, ICSA-17-031-01A BINOM3 Electric Power Quality Meter (Update A), February 7, 2017
- MedSec Holdings, ICSMA-17-009-01A St. Jude Merlin@home Transmitter Vulnerability (Update A), February 6, 2017
- Maxim Rupp, ICSA-17-033-01 Honeywell XL Web II Controller Vulnerabilities, February 2, 2017
- Brian Gorenc and Juan Pablo Lopez working with Trend Micro's Zero Day Initiative, ICSA-17-031-02 Ecava IntegraXor, January 31, 2017
- Maxim Rupp, ICSA-17-026-01 Eaton ePDU Path Traversal Vulnerability, January 26, 2017
- Davy Douhine of RandoriSec, ICSA-17-026-02 Belden Hirschmann GECKO, January 26, 2017
- Ruslan Habalov and Jan Bee of the Google ISA Assessments Team, ICSA-17-024-01 Schneider Electric Wonderware Historian, January 24, 2017
- Mohammed Shameem, ICSA-17-019-01 Schneider Electric homeLYnk Controller, January 19, 2017
- Tenable Network Security, ICSA-17-012-01 Advantech WebAccess, January 12, 2017
- Juan Pablo Lopez Yacubian, ICSA-17-012-02 VideoInsight Web Client, January 12, 2017
- Karn Ganeshen, ICSA-17-012-03 Carlo Gavazzi VMU-C EM and VMU-C PV, January 12, 2017
- Vint Maggs from Savannah River Nuclear Solutions, ICSA-17-010-01 OSIsoft PI Coresight and PI Web API, January 10, 2017
- Alexey Osipov and Ilya Karpov of Positive Technologies, ICSA-16-336-06 Rockwell Automation MicroLogix 1100 and 1400 Vulnerabilities, January 5, 2017

Upcoming Events

April 2017

ICSJWG 2017 Spring Meeting

April 11–13, 2017

Minneapolis, Minnesota

Event description and redistration

June 2017

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

Date TBD

Idaho Falls, Idaho

Course description

Registration with be posted mid-March

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.

PCII Protection – Your Information Will Be Protected

Industry partners may request protection under the Critical Infrastructure Information Act of 2002 when submitting information to ICS-CERT. If the proper process is followed and ICS-CERT validates that information, it becomes PCII. ICS-CERT's policy is to keep confidential any reported information specific to your organization or activity. Protected Critical Infrastructure Information (PCII) protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data. PCII can only be accessed in accordance with strict safeguarding and handling requirements. Only trained and certified federal, state, and local government employees or contractors may access PCII. (http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program).

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.

Report an incident.

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.

ICS-CERT publishes the ICS-CERT Monitor bimonthly, six times a year.

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.