ICS-CERT MONTHLY MONITOR

February 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

NOTEWORTHY INCIDENTS IN JANUARY

SITUATIONAL AWARENESS

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

Contact Information

For any questions related to this report or to contact ICS-CERT:

E-mail: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

For Control Systems Security Program (CSSP) Information and Incident Reporting:

http://www.ics-cert.org

NOTEWORTHY INCIDENTS IN JANUARY

GOVERNMENT FACILITIES SECTOR

In January, ICS-CERT identified and responded to a cyber intrusion into a building Energy Management System (EMS) used to control heating and cooling for a state government facility. The incident and facility were identified by ICS-CERT after correlating a variety of information posted in open sources.

ICS-CERT established contact with the facility and informed them of open source posting of their information. Facility personnel reported to ICS-CERT that they had discovered unauthorized adjustments to the EMS control settings that had resulted in unusually warm temperatures in the facility. Concerned about this anomalous activity, quick thinking personnel had reset the system settings to normal values and had adjusted the configuration to remove the Internet accessibility. They also preserved all available logs from the time of the incident and provided them to ICS-CERT for further analysis.

ICS-CERT analyzed the provided telemetry data and access logs and determined that temperature set points had been changed by an unauthorized user via the Internet accessible interface. Someone had gained access to this system despite the remote logon configuration requiring a password.

ICS-CERT strongly recommends that asset owners and operators audit their configurations for Internet accessibility, regardless of whether they believe they have Internet accessible devices. Often, control systems are found to have Internet accessible devices installed, of which the asset owners and operators are unaware. These situations pose an increased risk of attack to those systems.

ICS-CERT has issued several alerts concerning the risk introduced by maintaining Internet accessible control system devices. For more information on Internet accessible control systems, see ICS-CERT alert titled

"ICS-ALERT-11-343-01—Control System Internet Accessibility," published on December 09, 2011.

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT at ICS-CERT@dhs.gov or 1-877-776-7585.

SITUATIONAL AWARENESS

SNORT IN AN ICS ENVIRONMENT

Much ado has been made of the disclosure of PLC vulnerabilities by the Project Basecamp team at the S4 conference in January 2012. Nearly as much has been made about those bugs discovered by Billy Rios and Terry McCorkle in the ICS software—primarily HMIs—that they evaluated in their free time for the 100 days of SCADA bugs presentation at DerbyCon 2011. Finally, following closely on the heels of the vulnerability disclosures, ICS-CERT issued an alert on February 3, 2012, about SSH brute force scanning against critical infrastructure.

This combination of events further highlights the need to detect and respond to attacks against critical infrastructure. Unfortunately, it is well known that a gap exists between ICS cyber defenses and adversarial capabilities.

To address the immediate need for situational awareness of potential threats, ICS-CERT has evaluated available research on control system networks incident detection and Network-based Intrusion Detection System (NIDS) technology. The National Electric Cyber Security Organization (NESCO) and the Open Information Security Foundation (OISF) announced that they will be supporting updates for the NIDS preprocessors specific to ICS protocols, which were originally written by Digital Bond. The effort will focus on the updates necessary for SNORT and Suricata, both open source NIDS packages, to function effectively in ICS environments.

Why is this significant? Up to this point, a major obstacle for ICS security teams has been how to test and deploy IT security tools in the ICS space. In many cases, this simply hasn't been possible because of ICS operational needs and the legacy technology used in many ICS environments. Now, the open-source IT security research community has paired up with ICS security teams, DHS, NESCO, and other stakeholders to research specific ICS network threats and produce tools to address them.

NIDS Support for ICS Environments:

SNORT 2.9.2.1 was released on January 19, 2012, and included the upgraded preprocessors, allowing ICS integrators and implementers to detect incidents running against ICS network resources or communications protocols. No date for the Suricata preprocessor updates has been published at this time; although the updates were scheduled for OISF discussion on February 7, 2012.

NIDS signatures for common network protocols, such as DNP3, Modbus TCP, and EtherNet/IP, as well as a range of vulnerability signatures, can be downloaded from the Digital Bond website for use with SNORT, Suricata, or other NIDS products that can import NIDS signatures in the SNORT format.

Or, when deploying a NIDS in the ICS environment isn't possible, a NIDS system can be deployed at the junction of the corporation and control system network. Because most major NIDS applications can consume rule sets in the SNORT format, it is possible to deploy a sensor with the ICS rule sets at the corporate/control system or DMZ/control system junctions without disrupting operational network communications. This would provide some level of visibility into the health, status, etc. of the control system network communications without the fear of service interruption or network throttling. Digital Bond has a link to the SNORT preprocessors and rule sets available for download on its QuickDraw IDS web page. They also have identified a number of major IT security companies whose NIDS applications can import the ICS rules if the new, ICS deployment needs to be shoe-horned off an existing NIDS deployment.

Documentation and Research Resources:

Haven't deployed a NIDS in an ICS environment before? More and more documentation is available from a number of sources, outlining specifics of how to plan NIDS deployments in ICS networks. ICS-CERT has compiled a preliminary list of NIDS-ICS resources for customers and industry partners who are considering a NIDS deployment. This list is not comprehensive, but it contains information regarding needs assessments, architectural planning, and common obstacles others have found when deploying NIDS in process control networks.

Manuel Humberto Santander Peláez's, a security expert working for a utility company and a SANS Internet Storm Center handler, post on the SANS Internet Storm Center regarding SNORT 2.9.2.1, http://isc.sans.edu/diary.html?storyid=12346

Overview of the SNORT release and its impact on the SCADA world, http://www.infosecisland.com/blogview/19649-Snort-and-SCADA-Protocol-Checks.html

NIST's recommendations for acquiring and deploying an IDS system, http://csrc.nist.gov/publications/nistbul/itl99-11.txt

A second post by Manuel regarding the need for security in an ICS environment, http://isc.sans.edu/diary.html?storyid=9436

Patrick Weaver's reference on the SNORT website for using SNORT to meet NERC CIP requirements, http://www.snort.org/assets/114/Snort_RH5_SCADA.pdf

Digital Bond's QuickDraw IDS portal, which requires subscription to the portal to view the documentation but is free to the public, contains a variety of documentation regarding NIDS needs and deployment requirements in an ICS environment, http://www.digitalbond.com/tools/quickdraw

Industrial Defender's NIDS portal, which requires subscription to the portal to view the documentation but is free to the public, contains a variety of documentation regarding NIDS needs and deployment requirements in an ICS environment, http://www.industrialdefender.com/products/supported/nids.php

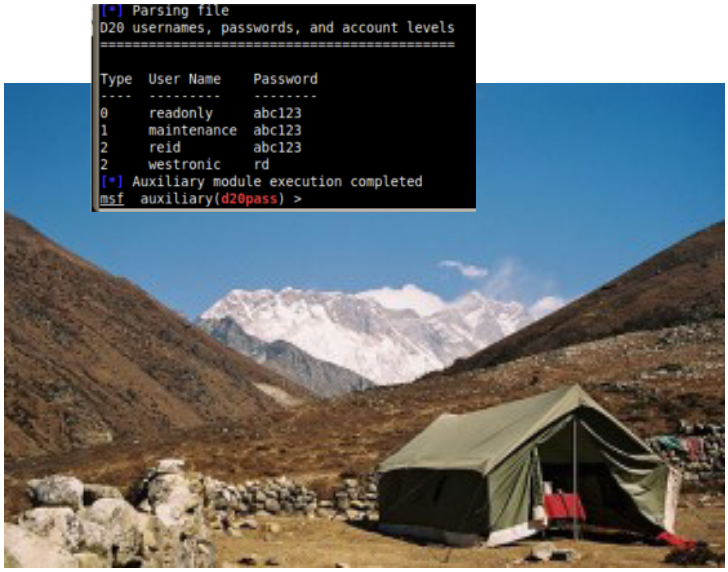
As always, feel free to contact the ICS-CERT team if you have any questions or need further information regarding ICS security concerns or incidents.

PROJECT BASECAMP

Project Basecamp was a research project by a six person team for the S4 2012 conference, which was held in January 2012. The Project Basecamp team performed vulnerability assessments on seven different programmable logic controller (PLC) products from major vendors and provided those results to Digital Bond. Siemens PLCs were not included in this review as the team wanted to focus on other, popularly deployed products that have not received the same level of scrutiny that Siemens devices have since the discovery of Stuxnet. The products tested for Project Basecamp were:

- General Electric D20ME
- Schneider Electric Modicon Quantum
- RA Allen-Bradley ControlLogix
- RA Allen-Bradley MicroLogix
- Koyo/DirectLOGIC H4-ES
- Schneider Electric/Control Microsystems SCADAPack
- Schweitzer SEL-2032.

Each of the five volunteer researchers (Dillon Beresford, Jacob Kitchel, Ruben Santamarta and two anonymous researchers) was assigned a single PLC to test for the project and Reid Wightman,



(Courtesy of Dale G. Peterson's Project Basecamp at S4)

a Digital Bond employee, evaluated the remaining two. The researchers used standard penetration testing and reverse engineering techniques against the PLCs to see how systems withstood known attack techniques. In many cases, the team was able to identify a number of mechanisms by which attackers could use known techniques to acquire user credentials, interrupt processes, or execute arbitrary code on the PLCs. The results of the testing were presented for the first time at the S4 conference. Videos of the presentations and technical details regarding the results can be viewed on the Digital Bond Project Basecamp webpage.

Impact of Successful Attacks

Digital Bond has published information regarding vulnerabilities specific to some of the seven PLCs evaluated and a number of stand-alone tools that can be used to identify vulnerable systems. The company has also worked with Rapid 7s research team to develop Metasploit Framework exploit modules that can be used to determine how much and what kind of impact active exploitation of the vulnerabilities would have on each of the PLCs. Plug-ins for the Nessus vulnerability scanner have also been released for those who require a less invasive identification mechanism for the vulnerabilities.

As anticipated, the range of vulnerabilities discovered on the test systems, the types of exploitation techniques that could be used successfully against the various PLCs, and the impact to each device varied greatly. In some cases, the PLC itself could be forcibly rebooted, interrupting all processes the PLC managed. In others, the network stack on the device could be tipped over, causing disruption of all network communications to and from the device. One attack resulted in the acquisition of legitimate credentials, i.e., unauthorized, remote access with administrative privilege, allowing the researcher to manipulate the PLC's ladder logic. Another exploitation technique allowed the researcher to gain root access to command shells on the systems.

Finally, and perhaps most importantly, evaluation of the ControlLogix PLC resulted in successful exploitation of not just the PLC but of the EtherNet/IP protocol itself. Rubén Santamarta, an independent researcher on the Project Basecamp team, outlined several ways to exploit both the EtherNet/IP communications protocol and the ControlLogix network stack in his "Attacking ControlLogix," presentation. Architectural design issues within the EtherNet/IP protocol itself can be exploited to either stop the PLC CPU altogether or forcibly reboot the Ethernet controller. Attacks against the ControlLogix network stack were discovered to generate similar results.

What is most significant about Santamarta's report was the exploitation of the EtherNet/IP protocol itself. Digital Bond's assessment of the flaw indicates the protocol may be exploitable in deployments using PLCs other than the ControlLogix system tested by Santamarta. Further research will be required to verify whether this is indeed the case.

Mitigation Needs

While a number of the vulnerabilities discovered by the Project Basecamp team have been addressed in ICS-CERT alerts or advisories, these flaws cannot be remediated until the vendors issue upgrades to address them. Those who are responsible for securing vulnerable EtherNet/IP implementations will need to deploy compensating controls and detection mechanisms until the design issue is resolved or handled by individual vendors in PLC network stack updates.

At best, groups that have deployed these PLCs will need to deploy compensating controls in order to:

1. Identify potentially vulnerable systems and baseline how they can be accessed from the control system and corporate networks via remote administration tools or the public Internet
2. Detect unauthorized use of, illegitimate access to, or unauthorized change of all credentials on the PLCs
3. Restrict use of or access to web servers that provide remote management capabilities
4. Detect possible attacks using the Metasploit and Nessus modules against vulnerable devices or network communication protocols.

TARGETING SOURCE CODE

Few people, if any, have missed the upward swing of highly sophisticated, targeted attacks against critical infrastructure and government organizations. Nor have many people missed that adversaries have added a new goal, data exfiltration, to their attack scenarios. One of the less publicized trends has been the exfiltration of source code as a result of such attacks.

Consider, however, the number of successful attacks in which attackers demonstrated access to or are believed to have had access to source code repositories.

According to recent reports, a hacktivist group recently acquired source code for two Symantec products, Norton Antivirus and pcAnywhere. The group released source code for pcAnywhere, a remote administration tool that is used widely across ICS networks, in early February, after Symantec refused to pay $50,000 to the group.

A hacktivist[a] group leaked source code in June 2011 for the Sony Computer Entertainment Developer Network, a website that is used to store all the developer tools and kits for Sony products including PlayStation 3, PSP, Blu-Ray, etc.

Operation Aurora, reported in January 2010, reputedly affected not only Google but Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical. According to the McAfee research team, the attack deliberately targeted source code repositories and had the ability to alter the code base if they so desired.

If trends in targeted attacks against critical infrastructure continue to mirror the trends of targeted attacks against IT infrastructure, ICS security teams should expect that source code will become an increasingly valuable target. From the attacker's perspective, source code is interesting because it can be used to provide both technical and competitive advantage.

1. Competitive advantage—An attacker can use the application source code for any product deployed in a target environment to ensure long-term access to competitors' data or resources by using the source code as a 0-day vulnerability or exploit "map." Access to source code can also help competitors leapfrog past the target by using the target data to speed their own product development lifecycle.

2. Ensure long-term access—Software re-use is a common practice when developers create new applications. Legacy applications typically retain large chunks of old code for functionality and backwards compatibility. An attacker with source code to study could have access to an application for years after the source code has been acquired since old code doesn't die easily.
3. Mask attacker's access—An attacker with access to source code has time to find exploits that will allow the unauthorized access to appear legitimate, making successful attacks difficult, if not impossible, to detect.

Why is this relevant to control system security teams?

1. Supply chain poisoning—Imagine that Vendor A provides an application that is deployed extensively in ICS networks. Now imaging that a sophisticated threat actor acquires the source code, modifies certain portions to create malicious results, and quietly introduces the modified code base to the Vendor

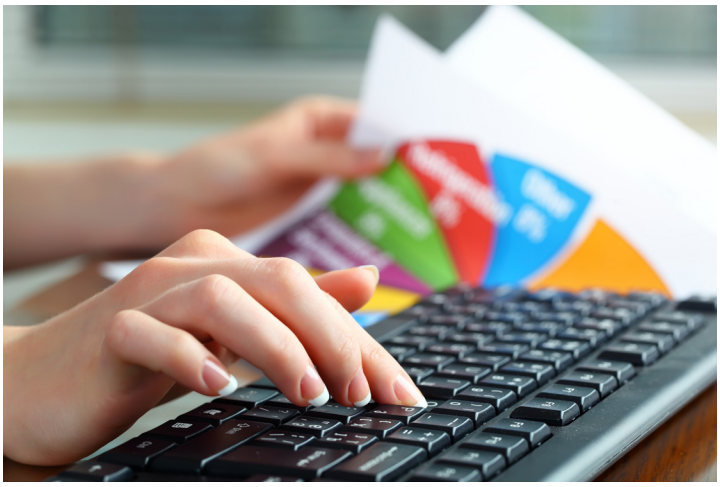
a. Hacktivist groups are ideologically motivated hackers who attack entities; networks to promote change or make a political statement. Tactics inlclude web defacements, redirects, denial of service, information theft, website parodies, virtual sit-ins, and virtual sabotage. Some groups are well organized and aim to conduct more malicious attacks to advance their views.

A network. The supply chain has been poisoned and future installations of the Vendor A application will have malicious content that could cause any number of problems.

2. Exploiting vulnerabilities—Suppose a threat actor acquires the Vendor A application source code and identifies all the vulnerabilities. The actor could then develop exploits against any number of those vulnerabilities and leverage that knowledge to attack the Vendor A installed customer base. Vendor A would have to identify and also to resolve each exploitable vulnerability in the code base to protect its customers. This is particularly significant given the sheer amount of software each ICS vendor appears to support and the length of time a new device is expected to perform. Attackers who gain access to ICS source code could potentially use that source code to derive new attacks for decades after it is acquired.
3. Staged attacks (aka "Man-in-the-Middle" scenarios)—Integration of third-party services and technology is a common phenomenon in the ICS world. This also means ICS operators take a critical dependency on a third party whose network and resources may or may not be well secured. Should the source code or application base of a trusted third party be compromised, the operator would be dependent on the third party or integrator to detect the compromise and notify them of it. In staged attacks that leverage trusted services or resources, incident response teams generally do not identify anomalous activity as malicious until after the impact has occurred. Attackers typically leverage third-party access to launch attacks from outside the target network and hide activity under the guise of trusted, legitimate activity.
4. Localized source code—Control systems inherently require customization through ladder logic, configuration changes, etc. for each installation. Any piece of this information should be considered a high value target from both a technical and business perspective. Technically, acquisition of localized source code would increase an attacker's efficiency during an system disruption. Organizationally, uncontrolled or unauthorized disclosure of data such as intellectual property, process data, or billing information can present significant financial, strategic, legal, or regulatory/compliance risks.

GETTING STARTED "SECURING INDUSTRIAL ASSETS"

Over the past year significant discoveries in the areas of adversarial capabilities have identified that many companies across the 18 critical infrastructure and key resources (CIKR) are struggling to cope with the growing threat toward their industrial assets. Significant efforts have been taken in industry and government to improve awareness and capability to defend critical assets from cyber intrusions and potential attacks. The Department of Homeland Security Control Systems Security Program (CSSP), along with standards organizations, has provided baseline standards and approaches to securing industrial assets. The amount of information generated makes it difficult to know where to start. The following strategies are recommended to aid asset owners and operators with getting started.



The first step to understanding the organization's overall security posture is to fully understand the current state. ICS-CERT recommends the CSET Assessment tool, available at http://www.us-cert.gov/control_systems/satool html.

Onsite assessment assistance is available through the CSSP. This will help the organization understand the current security posture in relation to industry standards and to develop a gap analysis result.

The next step is to develop your knowledge base on recommended practices and related industry standards. ICS-CERT recommends reviewing the CSSP Introduction to Recommended Practices available at http://www.us-cert.gov/control_systems/practices/.

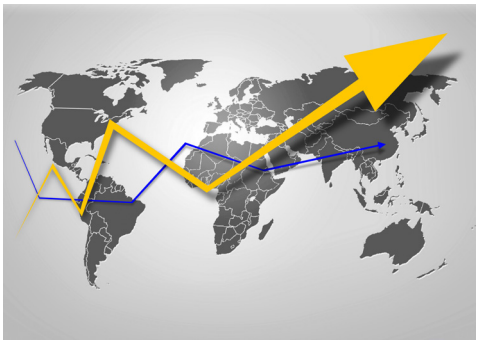
Develop a work plan and procurement plan that enables closing the gap and implementing sound practices toward securing control system networks. For procurement, ICS-CERT recommends the Cyber Security Procurement Language for Control systems

SITUATIONAL AWARENESS (Continued)

available at http://www.us-cert.gov/control_systems/csdocuments html

The references and standards available to asset owners and operators are there to aid in establishing a baseline level of security that is widely acceptable by industry experts operating in the cyber security fields with existing and available technology and strategies. In no way do they ensure that the strategies and technology will be resilient against emerging threats that may work to defeat the accepted strategies and technology. Threat actors commonly focus on defeating existing security features and strategies and develop sophisticated means to do so.

Because of sophisticated attack strategies by threat actors, companies should adopt a cybersecurity improvement program that focuses on emerging threats and employee training. A reliance on the standards and recommended practices alone will not afford adequate protection against emerging threats as the threats are dynamic and changing. The Standards and references are snap shot moments in time addressing known threats and at-time known emerging threats. References and standards will contain some level of uncertainty and error depending on available information, time from publishing, and will always lag the threat capabilities.



RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-12-020-01 -S4 Disclosure of Multiple PLC Vulnerabilities in Major ICS Vendors"

Alert "ICS-ALERT-12-020-02-Rockwell Contrologix PLC Multiple Vulnerabilities"

Alert "ICS-ALERT-12-020-03-Schneider Modicon Multiple Vulnerabilities"

Alert "ICS-ALERT-12-020-04 - Schweitzer SEL-2032 Plaintext Service Crash"

Alert "ICS-ALERT-12-020-05 - Koyo ECOM100 Multiple Vulnerabilities"

Alert "ICS-ALERT-12-020-06 - Wellintech KingSCADA Insecure Password Encryption"

Alert "ICS-ALERT-12-020-07 - WAGO - IO 750 Multiple Vulnerabilities"

Alert "ICS-ALERT-12-019-01-GE D20ME PLC Multiple Vulnerabilities"

Alert "ICS-ALERT-12-017-01-Rockwell Automation FactoryTalk RNADIAGRECEIVER"

ADVISORIES

Advisory "ICSA-12-026-01 - Siemens SIMATIC WinCC vulnerabilities"

Advisory "ICSA-12-012-01A - Open Automation Software OPC Systems .Net Vulnerability"

Advisory "ICSA-12-024-02 - MICROSYS, SPOL. S R.O. Promotic Multiple Vulnerabilities"

Advisory "ICSA-12-024-01 - Ocean Data Systems Dream Reports XSS and Write Access Violation Vulnerabilities"

Advisory "ICSA-12-018-02 - Certec Atvise Server Remote DOS"

Advisory "ICSA-12-018-01 - Schneider Ethernet Module Hard Coded Credentials"

Advisory "ICSA-12-016-01 - CogentDataHub XSS and CRLF"

Advisory "ICSA-11-353-01 - 7-Technologies Interactive Graphical SCADA"

Advisory "ICSA-12-012-01 - Open Automation Software OPC Systems .Net Vulnerability"

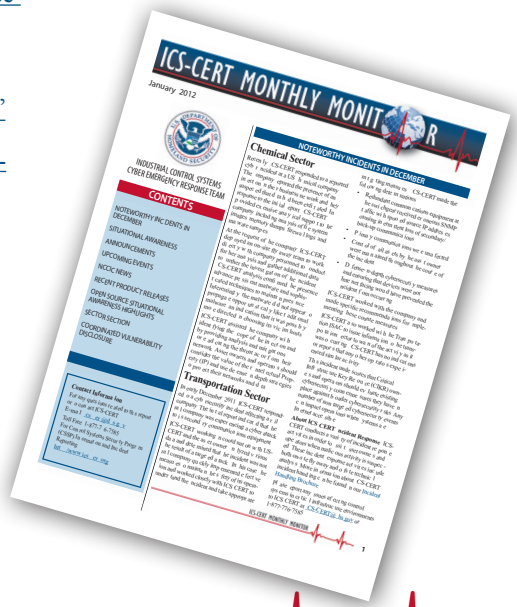
Advisory "ICSA-12-006-01 - 3S Smart Software Solutions CoDeSys Vulnerabilities"

Advisory "ICSA-11-343-01 - Siemens FactoryLink Multiple ActiveX Vulnerabilities"

Advisory "ICSA-11-332-01A - Invensys Wonderware InBatch ActiveX Vulnerabilities"

OTHER

The ICS-CERT Monthly Monitor January 2012 issue includes highlights of activities from December 2011.


ICS-CERT MONTHLY MONITOR

January 2012

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CONTENTS

NOTEWORTHY INCIDENTS IN DECEMBER

SITUATIONAL AWARENESS

ANNOUNCEMENTS

UPCOMING EVENTS

NCCIC NEWS

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

SECTOR SECTION

COORDINATED VULNERABILITY DISCLOSURE

NOTEWORTHY INCIDENTS IN DECEMBER

Chemical Sector

Transportation Sector

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

ICS-CERT compiles this section from multiple resources including current events as disclosed on websites, blogs, mailing lists, and at conferences. ICS-CERT does not endorse the opinions or comments stated in these articles, nor has the US Department of Homeland Security (DHS) independently verified the technical information included. The links provided were confirmed at the time of data capture. ICS-CERT is not responsible for broken or nonfunctioning URLs.

Researchers Postpone Release Of Free Smart Meter Security Testing Tool

2012-01-31

Looking into the Eye of the Meter – Don C. Weber

When you look at a Smart Meter, it practically winks at you. Their IR port calls to you. It calls to criminals as well. But how do criminals interact with it? We will show you how they look into the eye of the meter. More specifically, this presentation will show how criminals gather information from meters to do their dirty work. From quick memory acquisition techniques to more complex hardware bus sniffing, the techniques outlined in this presentation will show how authentication credentials are acquired. Finally, a method for interacting with a meter's IR port will be introduced to show that vendor specific software is not necessary to poke a meter in the eye.

http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/232500808/

Anatomy of a Vulnerability: Modicon Quantum

2012-01-31

In addition to having a slew of backdoor accounts, an open telnet service, and an open WindRiver RPC-Debug service open on this device, it has an unsigned firmware, managed accounts that are stored with usernames and passwords in plaintext, and buffer overflows galore.

http://www.digitalbond.com/2012/01/31/anatomy-of-a-vulnerability-modicon-quantum/

Exelon shuts Byron nuclear plant unit after power loss

2012-01-30

A nuclear reactor at a northern Illinois plant shut down Monday after losing power, and steam was being vented to reduce pressure, according to officials from Exelon Nuclear and federal regulators. Unit 2 at Byron Generating Station shut down around 10:18 a.m., after losing power from an off-site source, Exelon officials said. Diesel generators began supplying power to the plant equipment and operators began releasing steam from the non-nuclear side of the plant to help cool the reactor, officials said.

http://www.chicagobusiness.com/article/20120130/NEWS11/120139975/

SCADA Systems in Railways Vulnerable to Attack

2012-01-25

Reports of a possible cyber-attack against a rail company highlight the issues of protecting industrial control systems that keep the country's critical infrastructure running.

http://www.eweek.com/c/a/Security/SCADA-Systems-in-Railways-Vulnerable-to-Attack-124045/

http://www.wired.com/threatlevel/2012/01/railroad-memo/

10K Reasons to Worry About Critical Infrastructure

January 24, 2012

A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices.

http://www.wired.com/threatlevel/2012/01/10000-control-systems-online/

Hackers manipulated railway computers, TSA memo says

2012-01-23

Hackers, possibly from abroad, executed an attack on a Northwest rail company's computers that disrupted railway signals for two days in December, according to a government memo recapping outreach with the transportation sector during the emergency.

http://www.nextgov.com/nextgov/ng_20120123_3491.php

http://news.techeye net/security/hackers-hijack-us-trains

http://www.ibtimes.co.uk/articles/286628/20120124/computer-hackers-hijack-trains-tsa-memo.htm

Open Automation Software plugs DoS flaw in ICS application

2012-01-13

Open Automation Software has issued a patch for a vulnerability to its OPC Systems.NET industrial control system (ICS) application that could be used for a denial of service (DoS) attack.

http://www.infosecurity-magazine.com/view/23217/

Latest Snort provides alarm for industrial control systems

January 11, 2012

Version 2.9.2 of open source network intrusion detection system (NIDS) Snort has been released with new preprocessors that add support for protocols used in industrial control systems. The additional functionality should allow Snort to detect targeted attacks on networked SCADA systems.

http://www.h-online.com/security/news/item/Latest-Snort-provides-alarm-for-industrial-control-systems-1406990.html

China Not The U.S.'s Only Cyber-Adversary

2012-01-11

China long has been the focus of U.S. authorities and security researchers as a major source of cyber espionage against the U.S., but potential new evidence of targeted attacks by India against the U.S. demonstrates just how widespread cyberspying might be.

Even with increasing questions today surrounding the authenticity of a purported Indian military document leaked by a group

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

of self-professed Indian hackers who claim to be part of the Anonymous hacktivist movement in the wake of an investigation into whether India pilfered emails from the U.S.-China Economic and Security Review Commission, the events have spurred discussion about cyber espionage by nations other than China, which has been synonymous with the advanced persistent threat (APT).

http://www.darkreading.com/advanced-threats/16701091/security/attachs-breaches/232400208/

Feds Seek Stronger Security For Power Grid

2012-01-10

The Department of Energy (DOE) and the Department of Defense (DHS) have teamed up to create a cybersecurity model that can be tested and applied across the utility industry to provide insight into how to better protect the U.S. electricity grid.

The Electric Sector Cybersecurity Risk Management Maturity Model pilot project aims to work with experts in both the public and private sector to use existing cybersecurity strategies to develop a so-called "maturity model" that can identify how secure the electricity grid currently is from cyber threats, according to a White House blog post by White House cybersecurity coordinator Howard Schmidt. It will then test that model with participating utility companies to see how well it works, he said.

http://www.informationweek.com/news/government/security/232400080

GSA seeks proof of systems security from vendors

January 09, 2012

The General Services Administration wants more proof its vendors are securing the agency's systems — and GSA is not just stopping at the prime contractor level.

http://www.federalnewsradio.com/241/2695517/GSA-seeks-proof-of-systems-security-from-vendors

Smart Grid Security Inadequate, Threats Abound

2012-01-04

Near chaos. That's the current state of security for smart grids, according to Pike Research. A recent report by the research firm finds that a lack of security standards, a hodgepodge of products and increasingly aggressive malicious hackers will make 2012 a challenging year for securing smart grids. (A smart grid uses IT and smart meters in an effort to make electric utilities more efficient, reliable and sustainable.)

http://news.idg.no/cw/art.cfm?id=A127ABC9-B53E-AC90-3176B393E1D42341

UPCOMING EVENTS

MARCH

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)
March 12–16, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

APRIL

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)
April 9–13, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

MAY

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)
May 14–18, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

We Want to Hear from You

A key aspect of our mission is providing relevent and timely cybersecurity information products and services to 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 cn 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@dhs.gov.

DOCUMENT FAQ

What is the publication schedule for this digest?

ICS-CERT publishes the "ICS-CERT Monthly Monitor" approximately 12 times per year. Generally, each issue includes information collected in the previous 28 to 31 days.

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://www.us-cert.gov/control_systems/ics-cert/.

Please direct all questions or comments about the content, or suggestions for future content, to ICS-CERT at ics-cert@dhs.gov

What is ICS-CERT?

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to:

- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

The "ICS-CERT Monthly Monitor" offers a means of promoting preparedness, information sharing, and collaboration with the 18 critical infrastructure/key resource (CIKR) sectors. ICS-CERT accomplishes this on a day-to-day basis through sector briefings, meetings, conferences, and information product releases.

This publication highlights recent activities and information products affecting industrial control systems (ICS), and provides a look ahead at upcoming ICS-related events.

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. This coordinated disclosure process ideally allows time for a vendor to develop and release patches and for users to test and deploy patches prior to public disclosure of the vulnerability. While this process is not always followed for a variety of reasons, ICS-CERT continues to strive for 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@dhs.gov or toll free at 1-877-776-7585.

Notable Coordinated Disclosure Researchers in January 2012

ICS-CERT appreciates having worked through the coordinated disclosure process with the following researchers:

- Billy Rios, Terry McCorkle, Shawn Merdinger and Luigi Auriemma, ICSA-12-026-01 – Siemens SIMATIC WinCC vulnerabilities, January 30, 2012
- Luigi Auriemma, ICSA-12-012-01A – Open Automation Software OPC Systems .Net vulnerability, January 26, 2012 (uncoordinated – but validated)
- Luigi Auriemma, ICSA-12-024-02– MICROSYS, SPOL s r. o. Promotic Multiple Vulnerabilities, January 24, 2012 (uncoordinated – but validated)
- Billy Rios and Terry McCorkle, ICSA-12-024-01 – Ocean Data Systems Dream Reports XSS and Write Access Violation vulnerabilities, January 24, 2012
- Luigi Auriemma, ICSA-12-018-02– Certec Atvise Server Remote DoS, January 18, 2012
- Ruban Santamarta, ICSA-12-018-01 – Schneider Ethernet Module Hard Coded Credentials, January 18, 2012
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-016-01 – CogentDataHub XSS and CRLF, January 16, 2012
- Kuang-Chun Hung (Morgan) (ICST), ICSA-11-353-01 – 7-Technologies Interactive Graphical SCADA, January 16, 2012
- Luigi Auriemma(uncoordinated but validated patch), ICSA-12-012-01 – Open Automation Software OPC Systems .Net vulnerability, January 12, 2012
- Celil Unuver and Luigi Auriemma (uncoordinated but validated patch), ICSA-12-006-01 – 3S Smart Software Solutions CoDeSys vulnerabilities, January 06, 2012
- Kuang-Chun Hung (Morgan) (ICST), ICSA-11-343-01 – Siemens FactoryLink Multiple ActiveX vulnerabilities, January 04, 2012

Researchers Currently Working with ICS-CERT

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Luigi Auriemma	Joel Langill	Rubén Santamarta	Dillon Beresford	Eireann Leverett
Secunia	Yun Ting Lo (ICST)	Kuang-Chun Hung (ICST)	Terry McCorkle	Shawn Merdinger
Celil Unuver	Knud Erik Højgaard (nSense)	Billy Rios	Greg MacManus (iSIGHT Partners)	