ICS-CERT MONITOR

October/November/December 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

Contact Information

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

Email: ics-cert@hq.dhs.gov

Toll Free: 1-877-776-7585

For Control Systems Security Program (CSSP) Information and Incident Reporting: http://www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

INCIDENT RESPONSE ACTIVITY

MALWARE INFECTIONS IN THE CONTROL ENVIRONMENT

ICS-CERT recently provided onsite support at a power generation facility where both common and sophisticated malware had been discovered in the industrial control system environment. The malware was discovered when an employee asked company IT staff to inspect his USB drive after experiencing intermittent issues with the drive's operation. The employee routinely used this USB drive for backing up control systems configurations within the control environment.

When the IT employee inserted the drive into a computer with up-to-date antivirus software, the antivirus software produced three positive hits. Initial analysis caused particular concern when one sample was linked to known sophisticated malware. Following analysis and at the request of the customer, an onsite team was deployed to their facility where the infection occurred.

ICS-CERT's onsite discussions with company personnel revealed a handful of machines that likely had contact with the tainted USB drive. These machines were examined immediately and drive images were taken for in-depth analysis. ICS-CERT also performed preliminary onsite analysis of those machines and discovered signs of the sophisticated malware on two engineering workstations, both critical to the operation of the control environment. Detailed analysis was conducted as these workstations had no backups, and an ineffective or failed cleanup would have significantly impaired their operations.

With confirmation that the sophisticated malware existed on the two engineering workstations, attention shifted quickly to the remaining eleven operator stations in the control environment. Manual analysis using the known characteristics of the malware revealed no signs of the malicious software on these operator stations.

After the onsite visit, ICS-CERT had two primary goals for assisting the organization.

- Identify effective and safe cleaning procedures that could be used to remove the remaining malicious artifacts.
- Identify best practices to prevent and detect future malware infections in this organization's control environment.

ICS-CERT obtained a number of images and other artifacts for additional offsite analysis. The in-depth analysis of the two engineering workstations was critical in identifying safe and effective malware cleaning procedures. The cleaning procedures were developed in close coordination with the organization's control system vendor to ensure that it would not adversely impact the workstations.

While the implementation of an antivirus solution presents some challenges in a control system environment, it could have been effective in identifying both the common and the sophisticated malware discovered on the USB drive and the engineering workstations.

INCIDENT RESPONSE ACTIVITY

In addition to backing up the engineering workstation configuration files, the USB drive was also transporting malware. A good backup procedure should incorporate best practices for USB usage to ensure that malicious content is not spread or inadvertently introduced, especially in critical control environments. This procedure should include cleaning the USB device before each use or the use of write-once media such as CDs or DVDs.

The organization also identified during the course of the investigation that it had no backups for the two engineering workstations. Those workstations were vital to the facility operation and, if lost, damaged, or inoperable, could have a significant operational impact. The recommended practice is to maintain a system of "hot spares" or other effective backups for all critical systems.

The ICS-CERT report detailing the analysis and malware indicators was shared with members of the Control Systems Center on the US-CERT Secure Portal.

VIRUS INFECTION AT AN ELECTRIC UTILITY

In early October 2012, a power company contacted ICS-CERT to report a virus infection in a turbine control system which impacted approximately ten computers on its control system network. Discussion and analysis of the incident revealed that a third-party technician used a USB-drive to upload software updates during a scheduled outage for equipment upgrades. Unknown to the technician, the USB-drive was infected with a variant of the Mariposa virus. The infection resulted in downtime for the impacted systems and delayed the plant restart by approximately 3 weeks.

ICS-CERT continues to emphasize that owners and operators of critical infrastructure should develop and implement baseline security policies for maintaining up-to-date antivirus definitions, managing system patching, and governing the use of removable media. Such practices will mitigate many issues that could lead to extended system downtimes. Defense-in-depth strategies are also essential in planning control system networks and in providing protections to reduce the risk of impacts from cyber events.

For more information, visit http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf.

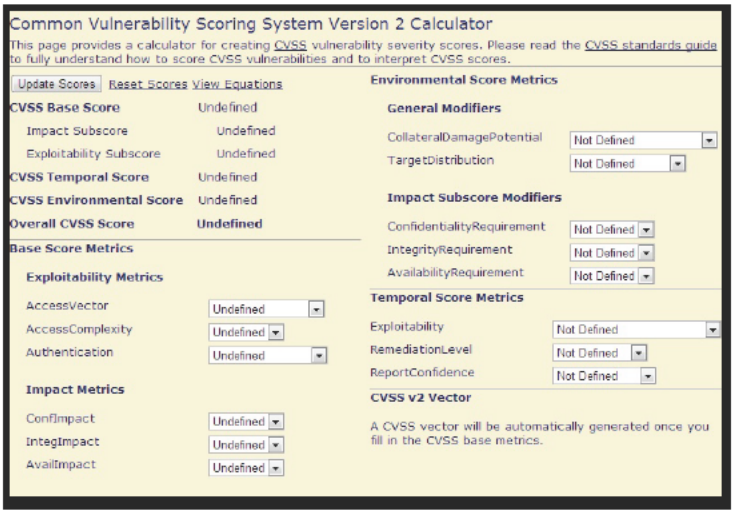
SITUATIONAL AWARENESS

A CLOSER LOOK AT CVSS SCORING

ICS-CERT continuously strives to improve its information products and now includes CVSS scoring to help readers assess the severity of reported vulnerabilities. ICS-CERT provides CVSS base scoring and the corresponding vector string for all vulnerabilities in published advisories. The CVSS score is an indicator of the severity ranging from 0, meaning no vulnerability present, up to 10, which indicates the highest severity vulnerability. ICS-CERT provides the base CVSS score in advisories as an indicator to asset owners and operators of the severity of the vulnerability. By providing the base metric, readers can use the base metric as a tool to quickly determine the seriousness of the vulnerability associated with the affected system. The asset owners and operators can use the base metric provided by ICS-CERT and apply the temporal and environmental metrics that are appropriate for their individual situation. Asset owners and operators typically use the total CVSS score to manage the risk of the vulnerability to assist in determining the priority for upgrading, applying compensating controls, or patching critical equipment.

About the CVSS Scoring System

The Common Vulnerability Scoring System (CVSS – see Figure 1) is used by ICS-CERT in vulnerability advisories. The CVSS base score is a ranking of the severity of the vulnerability on a scale of 0-10. The CVSS was originally commissioned by the National Infrastructure Advisory Council in support of the global Vulnerability Disclosure Framework to solve the problem of multiple incompatible vulnerability scoring systems. Since its



inception and adoption by the current maintainer, the Forum of Incident Response and Security Teams (FIRST), an upgraded version of CVSS is now commonly used. Version 2 was released in June 2007 to address issues such as inconsistencies in scoring methods. A number of CVSS score calculators are available online. Almost all vulnerabilities listed in the National Vulnerability Database (NVD) are associated with a corresponding CVSS base score to rank severity.

3 Parts of a CVSS Score

The total CVSS score is composed of three parts: base metrics, temporal metrics, and environmental metrics.

Base Metrics: The base metrics use the characteristics of the vulnerability that are constant with time and user environments. These variables include the access vector, access complexity, and authentication. They also take into consideration the vulnerabilities' impact to confidentiality, integrity, and availability. ICS-CERT recommends that control systems owners and operators customize the CVSS score by providing, when possible, temporal metrics as described below.

Temporal Metrics: The temporal metrics capture the threat of the vulnerability at a certain point in time. This metric is optional and will not affect the base score if not included.

Environmental Metrics: The final part of the CVSS score are the environmental metrics. These metrics take into account the unique environment to which the vulnerability affects such as the effect on an individual organization. This metric is also optional and may be excluded without bearing to the score if applied generically. ICS-CERT recommends that control systems owners and operators customize the CVSS score to their local environment by completing the environmental metrics as described below.

Customize CVSS Score to Local Environment

To calculate the scores, ICS-CERT uses the National Institute of Standards and Technology (NIST) NVD CVSS Version 2 concise score calculator found at: http://nvd nist.gov/cvss.cfm?calculator&adv&version=2. The base score is provided in the form of a CVSS vector string, which tells readers the variables that went into computing the score. An example of a vector string that equates to a base score of 10.0 is (AV:N/AC:L/Au:N/C:C/I:C/A:C). All advisories provide a link back to the NIST CVSS calculator that displays the base metrics (see Figure 2). Readers can combine information from the CVSS score, description of the vulnerability, and exploit availability and apply this information to the best of their ability to their individual operating environment. ICS-CERT provides CVSS base scores as a tool for affected asset owners to aid them in prioritizing their mitigation strategies. Control System owners/operators are encouraged to customize the *CVSS temporal and environmental metrics* to calculate a total score that applies to their individual deployment characteristics.

More information about CVSS scoring can be found at the FIRST CVSS website. Questions about how ICS-CERT implements CVSS can be obtained by emailing ICS-CERT at ics-cert@hq.dhs.gov.

VULNERABILITY OVERVIEW

USE OF HARD-CODED CREDENTIALS[c]

An attacker can log into the device using the hard-coded credentials that grant administrative access. Administrative credentials allow users to change device settings and read and write to the file system. This could result in a loss of confidentiality, integrity, or availability.

CVE-2012-4577[d] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[e]

b. Korenix, http://www.korenix.com, Web site last accessed October 23, 2012.
c. CWE, http://cwe.mitre.org/data/definitions/259.html, CWE-259: Use of Hard-coded Password, Web site last accessed October 23, 2012.
d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4577, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C), Web site last accessed October 23, 2012.

Figure 2

PROJECT SHINE

Using only their wits, an extensive list of control systems related search terms, a paper clip, and the Internet-facing device search engine SHODAN two researchers spear-headed an ambitious effort to compile a list of almost 500,000 devices with predicted control systems impact. Calling this effort Project SHINE (SHodan INtelligence Extraction), Bob Radvanovsky and Jake Brodsky of InfraCritical began using freely available tools in April 2012 to demonstrate the ease with which critical infrastructure devices can be discovered on the Internet. Bob approached ICS-CERT 6 months after the commencement of Project SHINE when the database consisted of approximately 460,000 IP addresses with more being added daily. Jake presented the research and reasoning behind Project SHINE at the October 2012 ICS Cyber Security Conference in Norfolk, Virginia.

According to the researchers, the purpose of Project SHINE is to raise awareness that many critical infrastructure assets are directly facing the Internet. In some instances, these devices have either

weak, default, or nonexistent logon credential requirements. As SHODAN is freely available, anyone with malicious intent could locate these devices and attempt logon, leaving these systems vulnerable to attack. Once accessed, these devices may be used as an entry point onto a control systems network, making their Internet facing configuration a major vulnerability to critical infrastructure. Working with government partners, ICS-CERT was able to categorize the IP addresses by sector types, sector organization names, and location information for each device and shortened the list to approximately 98,000 organizations within the United States. Further evaluation indicated that many of these logon sites were not directly associated with critical control devices and the list was again reduced to approximately 7,200 devices (See Figure 3) in the United States that appear to be directly related to control systems.

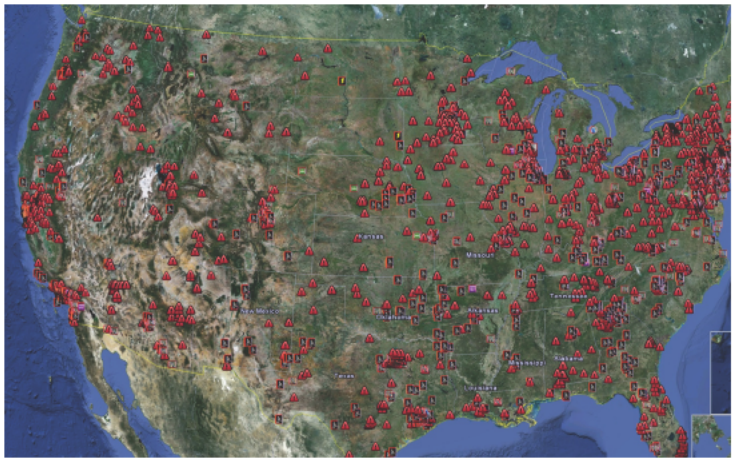


Figure 3. Approximately 7,200 Internet facing control system devices in the US.

The IP addresses located outside the US were parsed out by country and ICS-CERT leveraged CERT-to-CERT relationships, notifying international CERT/CIRT partners of the identified Internet facing devices in their respective countries. Over 100 countries have been notified, with additional notifications in process.

By examining the search terms used and the relevance to critical infrastructure, ICS-CERT has sorted the list by risk to critical infrastructure and is focusing on those devices that present the greatest vulnerability. ICS-CERT is working with a variety of private sector and government partners to identify the owners of the US-based devices on the list and to provide notification of the vulnerable configuration.

ICS-CERT recommends the following industry best practices in maintaining a minimal Internet facing footprint.

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Remove, disable, or rename any default system accounts wherever possible.
- Implement account lockout policies to reduce the risk from brute forcing attempts.
- Implement policies requiring the use of strong passwords
- Monitor the creation of administrator level accounts by third-party vendors.
- Adopt a regular patch life cycle to ensure that the most recent security updates are installed.

Additional information is available in the following documents to assist with securing critical infrastructure assets.

Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defensein-Depth Strategies.

ICS-ALERT-12-046-01A – (UPDATE) Increasing Threat to Industrial Control Systems.

ICS-CERT invites asset owners and operators as well as concerned parties in the control systems and critical infrastructure communities to contact ICS-CERT with any questions or concerns.

ACTION CAMPAIGN

ICS-CERT has been actively briefing critical infrastructure asset owners and stakeholders with essential information about increased and emerging cyber threats in an initiative called the "Action Campaign."

Throughout 2011 and 2012, intelligence, industry, and media reporting have all shown an increasing trend in cyber attacks targeted at energy and pipeline infrastructure around the world. ICS-CERT has been tracking threats and responding to intrusions into infrastructure such as oil and natural gas (ONG) pipelines and electric power organizations at an alarming rate. In 2012 alone, attacks against the energy sector comprised over 40% of all incidents reported to ICS-CERT. Many of these incidents targeted information pertaining to the ICS/SCADA environment, including data that could facilitate remote access and unauthorized operations. Other incidents involving highly destructive malware such as Shamoon, that reportedly targeted (but failed to impact) production networks of energy sector companies.[1]

[1] http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html

SITUATIONAL AWARENESS - Continued

In order to highlight the increased need for action, ICS-CERT partnered with DOE and other federal partners to kick off an Action Campaign consisting of regional classified (SECRET) and unclassified sessions to discuss recent attack campaigns aimed at the energy sector. These briefings have also included essential information regarding mitigation strategies, best practices, and emerging trends. The campaign was kicked off in early October and covered major markets across the US, including Arlington, Virginia; New York, New York; Washington, DC; Chicago, Illinois; Dallas, Texas; Denver, Colorado; San Francisco, California; Anchorage, Alaska; Houston, Texas; Atlanta, Georgia; and numerous others via secure video teleconferences (SVTC).

The Action Campaign briefings have provided actionable situational awareness to critical infrastructure and key resource (CIKR) asset owners and operators concerning sophisticated threat actors and their recent activities. Topics included:

- Recent cyber intrusion campaigns - an operational update on the ONG activity and other sophisticated intrusions that ICS-CERT has responded to in 2012.
- ICS vulnerabilities and exploits – The continued increase in vulnerability discovery as well as research studies into Internet facing ICS and the tools that exist to easily locate systems.
- Targeted malware such as Shamoon – its destructive nature and implications for US-based asset owners/operators
- Mitigations for asset owners – a discussion in how to combat targeted malware, 0-day exploits, sophisticated cyber intrusions, and the tools and resources available.

ICS-CERT also discussed the latest information about adversarial tactics and techniques and closed the discussions by providing detailed strategies and recommended practices for strengthening network security posture to allow for detection, prevention, and response to cyber intrusions by sophisticated threat actors. To date, these action campaign briefings have reached over 500 private sector attendees for the classified briefings and hundreds more for the unclassified briefings.

ICS-CERT recognizes that outreach activities in the form of risk and mitigation briefings play a key role in mitigating the overall risk to critical infrastructure. ICS-CERT will continue to conduct briefings on a regular basis to provide asset owners with the most up-to-date information on emerging threats and security measures that can be deployed to help thwart cyber attacks and reduce risk.

ICS-CERT NEWS

ICS-CERT – OPERATIONAL REVIEW FISCAL YEAR 2012

Incident Response

In 2012, ICS-CERT responded to a steady stream of cyber incidents, coordinated ICS vulnerabilities with vendors, and produced alerts and advisories to notify the ICS community of emerging cyber risks. These products provided information about attack techniques and indicators as well as mitigation strategies for reducing risks.

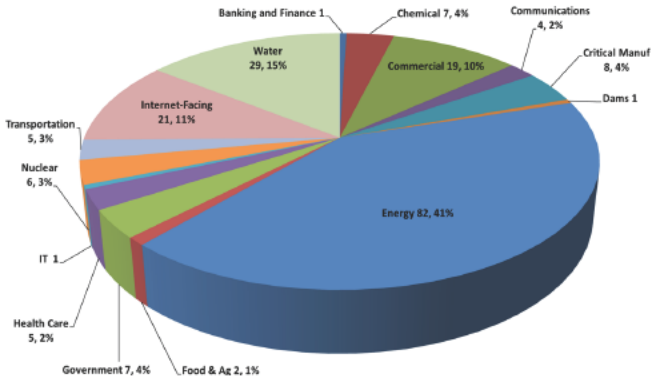


Figure 4. Incidents by Sector (+ Internet-Facing) – 198 Total in Fiscal Year 2012

*Fiscal year 2012 represents the time period of October 1, 2011–September 30, 2012

In fiscal year 2012,* ICS-CERT received and responded to 198 cyber incidents as reported by asset owners and industry partners. Attacks against the energy sector represented 41 % of the total number of incidents. Notably, ICS-CERT assisted 23 ONG sector organizations with incident response and recovery efforts following a targeted spear-phishing campaign. Analysis of the targeted systems indicated that information pertaining to the ICS/SCADA environment, including data that could facilitate remote unauthorized operations, was exfiltrated. ICS-CERT worked closely with many of the involved organizations and during the course of this response effort, analyzed over 50 malware samples and malicious files, 20 emails, and 38 hard drive images to determine the extent of the compromise and identify the techniques and tactics used the threat actors. ICS-CERT also deployed onsite incident response teams to assist 2 organizations that were compromised as a result of this campaign.

ICS-CERT continues to assist organizations with this campaign as well as other Advanced Persistent Threats (APT) activity affecting critical infrastructure. For more information about reducing risk and mitigating sophisticated attacks, visit ICS-CERT Technical Information Paper TIP -12-146-01A.

The water sector had the second highest number of incidents, representing 15% of all incidents across sectors. Spear phishing and Internet facing systems with weak or default credentials were the most common incidents in the water sector. Of note was a report of a water utility located in Springfield, Illinois (Curran-Gardner Public Water District) that was reportedly hacked from a IP address located in Russia. At the request of the utility and in coordination with the FBI, ICS-CERT deployed a fly-away team to the facility to interview personnel, perform physical and logical inspections of the control systems, and collect logs and artifacts for analysis. After detailed analysis of all available data, ICS-CERT and the FBI found no evidence of a cyber intrusion into the SCADA system of the water utility. ICS-CERT assesses that the pump failure was likely due to high mineral content that caused excessive wear. More information can be found at the ICS-CERT report on the incident.

ICS-CERT also responded to several cyber incidents impacting organizations in the nuclear sector. These organizations reported that their enterprise networks were compromised and in some cases, exfiltration of data occurred. In the cases of targeted attacks where lateral movement techniques could have been used by adversaries, ICS-CERT worked with the organizations to examine their network topologies, the interconnections between networks, and potential paths of compromise. Of the six incidents in the nuclear sector, ICS-CERT is not aware of any compromises into control networks.

Internet Facing ICS

Internet facing control systems devices were also an area of concern in FY 2012. ICS-CERT worked with a variety of researchers who used tools like SHODAN and ERIPP (Every Routable IP Project – Port80/TCP only) to identify and locate Internet facing control system devices that may be susceptible to compromise. One particular disclosure came from researcher Eireann Leverett, who used the SHODAN search engine to identify over 20,000 ICS-related devices that were directly IP addressable and vulnerable to exploitation through weak or default authentication. A large portion of the Internet facing devices belonged to state and local government organizations, while others were based in foreign countries. ICS-CERT worked with partners as well as 63 foreign CERTs in the effort to notify the identified control system owners and operators that their control systems/devices were exposed on the Internet.

Other disclosures came from Rueben Santamarta, Billy Rios, Terry McCorkle, Joel Langill, and other trusted sources.

ICS-CERT also issued alerts to urge the community to audit its control systems, regardless of whether they think they're connected to the Internet, to discover improperly configured systems and remove any default administrator level user names and passwords.

Vulnerability Coordination and Analysis

Vulnerability analysis and coordination activities also continued to increase, with more researchers leveraging ICS-CERT as a coordination vehicle to ICS vendors. In fiscal year 2012, ICS-CERT tracked 171 unique vulnerabilities affecting ICS products (see Figure 5). ICS-CERT coordinated the vulnerabilities with 55 different vendors. The total number of different vulnerabilities increased from FY 2011 to FY 2012, but buffer overflows still remained as the most common vulnerability type

Vulnerability Type	
Buffer Overflow	44
Input Validation	13
Resource Exhaustion	8
Authentication	8
Cross-site Scripting	8
Path Traversal	8
Resource Management	8
Access Control	7
Hard-coded Password	7
DLL Hijacking	6
SQL Injection	4
Credentials Management	3
Cryptographic Issues	3
Insufficient Entropy	3
Use After Free	3
Use of Hard-coded Credentials	2
Cross-Site Request Forgery	2
Privilege Management	2
Write-what-where Condition	2
Integer Overflow or Wraparound	2
Inadequate Encryption Strength	2
Missing Encryption of Sensitive Data	1
Code Injection	1
Forced Browsing	1
Miscellaneous	15
Total	171

Figure 5: Vulnerabilities by type, Fiscal Year 2012.

reported. In FY 2012, buffer overflow vulnerabilities composed 26 % of the reported vulnerabilities as compared to 46 % in FY 2011. ICS-CERT also noted an increase in vulnerabilities related to hardware, including ICS networking and medical devices. With the cases of coordinated disclosures and when appropriate, ICS-CERT provided analytic support to vendors in the form of proof-of-concept testing and patch validation to ensure that updates fully resolved the vulnerabilities.

Other noteworthy disclosures included the Project Basecamp research team who performed vulnerability assessments on seven different programmable logic controller (PLC) products from major vendors. 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 evaluated the remaining two. The researchers used standard security testing and reverse engineering techniques against the PLCs to demonstrate the fragility of the devices. 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.

Videos of the presentations and technical details regarding the results can be viewed on the Digital Bond Project Basecamp webpage. Digital Bond also developed Metasploit modules and Nessus plug-ins to help asset owners check for vulnerable configuration settings.

Other notable disclosures came from researchers Billy Rios and Terry McCorkle who identified multiple vulnerabilities in the Tridium Niagara AX Framework software. The vulnerabilities included directory traversal, weak credential storage, session cookie weaknesses, and predictable session IDs, all of which could be exploited remotely. The Tridium Niagara AX software platform integrates different systems and devices, e.g., HVAC, building automation controls, telecommunications, security automation, machine–to–machine (M2M), lighting control, maintenance repair operations (MRO), service bureaus, and facilities management.

The lengthy coordination of these and other vulnerabilities, led ICS-CERT to update its Vulnerability Disclosure Policy to set the expectation that ICS-CERT may disclose vulnerabilities 45 days after initial contact when vendors are unresponsive or unable to establish a reasonable timeframe for remediation (regardless of a vendor patch or workaround). The goal of this policy change is to balance the control system community's need for information about security vulnerabilities with the vendor community's need for time to respond effectively. The final vulnerability disclosure determination will be based on the best interests of the overall ICS community.

Information Products

Many of the resultant incident analysis and ICS vulnerabilities culminated in ICS-CERT alerts and advisories to the website and/or secure portal. In FY 2012, ICS-CERT published 332 information products, warning the ICS community about various threats and vulnerabilities that could impact control systems. As we move forward in 2013, ICS-CERT will continue to expand its capabilities and improve the services and information that it provides to critical infrastructure asset owners. A strong posture of continuous information exchange is essential to reducing cyber risks and improving the overall security posture of CIKR.

*F sca year 2012 represents the t me per od of October 1, 2011–September 30, 2012

ICSJWG FALL MEETING WRAP UP

The Department of Homeland Security conducted the Industrial Control Systems Joint Working Group (ICSJWG) 2012 Fall Meeting held October 15–18 in Denver, Colorado. Participation included 269 individuals from across the cybersecurity and ICS landscape. The meeting provided a unique opportunity for perspective sharing and partnering across all CIKR Sectors between federal agencies and departments as well as private asset owners/operators of ICSs.

Conference sessions included a broad range of topics to support the CIKR communities' ability to understand the current cybersecurity environment; knowledge sharing, assurance topics, real world examples of security applications, intrusion tactics and solutions, and a host of member selected subject matter. Many of the member selected topics delivered to overflow attendance as CIKR owners and operators took a deeper dive into other community member challenges and successes.

The motives and thought processes of hackers took center stage during the keynote address delivered by Billy Rios of Spear Point Security. Mr. Rios's compelling and sometimes humorous address compelled conference attendees to better understand the motivations behind those who discover and market exploits, take a closer look at cybersecurity methodology, and challenge the way owners and operators address threats to their systems. During the panel discussions, the conversations highlighted the challenges for CIKR communities to participate in cooperative initiatives to enhance cybersecurity posture across industry.

ICS-CERT appreciates the wide-ranging participation and contributions of presenters and attendees at the 2012 fall meeting. The open and honest discussions facilitated by this meeting are necessary as the ICSJWG community continues to evaluate the best approach to bring value to the CIKR community.

ICS-CERT NEWS - Continued

Many of the materials from the Industrial Control Systems Joint Working Group 2012 Fall Meeting in Denver, Colorado will be made available. Those presentations that are authorized for release are available at http://www.uscert.gov/control_systems/icsjwg/2012/fall/index.html, with links available for review and download.

Additional information including other submitted whitepapers and a complete compilation of presentations will soon be available on the site. Please monitor the page cited above for these documents' availability. This meeting was again noted as an exciting success because of the efforts and contributions of all the participants. To all the presenters and participants, thank you, for your support, and we look forward to the future contributions that you can make to the ICSJWG.

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-12-097-02A–(UPDATE) 3S-Software CODESYS Improper Access Control (2012-10-26)

ICS-ALERT-12-046-01A–(UPDATE) Increasing Threat To Industrial Control Systems (2012-10-25)

ICS-ALERT-12-284-01–Sinapsi eSolar Light Multiple Vulnerabilities (2012-10-10)

ICS-ALERT-12-277-01–Sielco Sistemi WinLog Lite SEH Overwrite Vulnerability (20121003)

ADVISORIES

ICSA-12-335-01—Post OAK Bluetooth Traffic Systems Insufficient Entropy Vulnerability (2012-11-30)

ICSA-12-325-01—Sinapsi Devices Multiple Vulnerabilities (2012-11-20)

ICSA-12-320-01–ABB AC500 PLC Webserver Buffer Overflow Vulnerability (2012-11-15)

ICSA-12-271-01–C3-ilex EOScada Multiple Vulnerabilities (2012-11-01)

ICSA-12-305-01–Siemens SiPass Server buffer overflow (2012-10-31)

ICSA-12-297-02–Korenix JetPort 5600 Hard-coded Credentials (2012-10-23)

ICSA-12-234-01–GE Intelligent Platforms Proficy Multiple Vulnerabilities (2012-10-15)

ICSA-12-283-01–Siemens S7-1200 Web Application Cross Site Scripting (2012-10-09)

ICSA-12-283-02–WellinTech KingView User Credentials Not Securely Hashed (2012-10-09)

ICSA-12-265-01–Emerson DeltaV Buffer Overflow (2012-09-28)

ICSA-12-271-02–Optimalog Optima PLC Multiple Vulnerabilities (2012-09-27)

ICSA-12-263-02–ORing Industrial Networking IDS-5042 Hard-Coded Credentails Vulnerability (2012-09-19)

ICSA-12-263-01–Siemens S7-1200 Insecure Storage of HTTPS CA Certificates-ICS-VU-268163 - Vulnerability in Siemens PLC (2012-09-19)

ICSA-12-262-01–Fultek WinTr SCADA (2012-09-18)

ICSA-12-256-01–Siemens WinCC WebNavigator Multiple Vulnerabilities (2012-09-12)

ICSA-12-150-01–Honeywell HMIWEB Browser Buffer Overflow (2012-09-17)

ICSA-12-251-01–RealWinDemo dll hijack (2012-09-07)

ICSA-12-249-03–Indusoft ISSymbol ActiveX Control Buffer Overflow (2012-09-05)

ICSA-12-249-02–WAGO IO 758 Default Linux Credentials (2012-09-05)

ICSA-12-249-01–Arbiter systems Power Sentinel Denial of Service Vulnerability (2012-09-05)

RECENT PRODUCT RELEASES

OTHER

JSAR-12-241-01B - (Update) Shamoon-DistTrack Malware (2012-10-16)

JSAR-12-241-01A - Shamoon-DistTrack Malware (2012-09-27)

The ICS-CERT Monthly Monitor September 2012 issue summarizes highlights of ICS-CERT activities from August 2012. (2012-10-10)

Follow ICS-CERT on Twitter: @icscert

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

New malware sneaks by most antivirus protection
2012-11-28

A recent study by University of Tel Aviv for Imperva comes to that conclusion, at least with regard to new viruses. The research team tested 82 new malware files against 40 antivirus products and found that the antivirus programs detected exactly none of them, TechWorld reports.

Even after giving the antivirus software additional chances at one-week intervals, the best of the antivirus products still took at least three weeks to detect the viruses, according to the report. And of the batch tested, Imperva said that two free programs, Avast and Emisoft, performed the best, along with McAfee antivirus.
http://gcn.com/blogs/pulse/2012/11/antivirus-0-for-82-against-new-malware.aspx
https://www networkworld.com/news/2012/112712-antivirus-software-a-waste-of-264547.html

U.N. atom agency says stolen information on hacker site
2012-11-27

The stolen information was contained in a statement by a group with an Iranian-sounding name calling for an inquiry into Israel's nuclear activities. The International Atomic Energy Agency (IAEA) is investigating Iran's nuclear program.
http://www reuters.com/article/2012/11/27/net-us-nuclear-iaea-hacking-idUSBRE8AQ0ZY20121127

Auto-Immune: "Symbiotes" Could Be Deployed to Thwart Cyber Attacks
2012-11-26

Anti-hacker defenses have long focused mainly on protecting personal computers and servers in homes and offices. However, as microchips grow smaller and more powerful, new targets for hackers are becoming widespread—embedded computers such as the electronics handling car engines, brakes and door locks; the routers that form the Internet's backbone; the machines running power plants, rail lines and prison cell doors; and medical devices such as defibrillators and insulin pumps. Many of these embedded devices can now link with other computers, putting them equally at risk to intruders. Indeed, in October, Secretary of Defense Leon Panetta warned that the U.S. faced the threat of a "cyber Pearl Harbor" if it failed to adequately protect these systems, echoing a warning CIA Director John Deutsch gave to Congress in 1996 about an electronic Pearl Harbor.

Now computer scientists are devising guardians they call symbiotes that could run on embedded computers regardless of the underlying operating systems. In doing so, they may not only help protect the critical infrastructure of nations and corporations but reveal that warfare against these devices may have been going on unseen for years, researchers say.
http://www.scientificamerican.com/article.cfm?id=auto-immune-symbiotes-could-be-deployed-to-thwart-cyber-attacks

Security firm showcases vulnerabilities in SCADA software, won't report them to vendors
2012-11-21

Malta-based security start-up firm ReVuln claims to be sitting on a stockpile of vulnerabilities in industrial control software, but prefers to sell the information to governments and other paying customers instead of disclosing it to the affected software vendors.

In a video released Monday, ReVuln showcased nine "zero-day" (previously unknown) vulnerabilities which, according to the company, affect SCADA (supervisory control and data acquisition) software from General Electric, Schneider Electric, Kaskad, Rockwell Automation, Eaton and Siemens. ReVuln declined to disclose the name of the affected software products.
…
"ICS-CERT has just contacted us some minutes ago requesting more details but we don't release information," Auriemma said. The vulnerabilities "are part of our portfolio for our customers so no public details will be released; they will remain private," he said.
http://www.goodgearguide.com.au/article/442632/

First graduate course in the nation dedicated to medical device security
2012-11-16

How do we begin to improve the information security of increasingly interconnected and wirelessly controlled medical devices? Starting with highly trained engineers who also appreciate the complexities of human factors and regulatory affairs. My upcoming Winter 2013 course at the University of Michigan on Medical Device Security will be the first of its kind in the nation to teach students about this topic. Students will learn the timeless concepts and cutting-edge skills in computer engineering, human factors, and regulatory policies that determine the safety and effectiveness of manufacturing software-controlled medical devices.
http://blog.secure-medicine.org/2012/11/first-graduate-course-in-nation.html

Help is available for effective continuous monitoring
2012-11-16

Fully continuous monitoring of the security status of information systems is an ideal that is unlikely to be reached because of the complexity of round-the-clock, real-time scanning of every aspect of a system. Both industry and government are moving toward making it more practical, however.
…
To help agencies get started, the National Institute of Standards and Technology is publishing guidance on continuous monitoring.
gcn.com/articles/2012/11/16/help-effective-continuous-monitoring.aspx
http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
http://csrc.nist.gov/publications/drafts/nistir-7800/Draft-NISTIR-7800.pdf

One Simple Trick Could Disable a City's 4G Phone Network
2012-11-15

High-speed wireless data networks are vulnerable to a simple jamming technique that could block service across much of a city, according to research findings provided to a federal agency last week.

The high-bandwidth mobile network technology LTE (long-term evolution) is rapidly spreading around the world. But researchers show that just one cheap, battery-operated transmitter aimed at tiny portions of the LTE signal could knock out a large LTE base station serving thousands of people. "Picture a jammer that fits in a small briefcase that takes out miles of LTE signals—whether commercial or public safety," says Jeff Reed, director of the wireless research group at Virginia Tech.
http://www.technologyreview.com/news/507381/one-simple-trick-could-disable-a-citys-4g-phone-network/

Top U.S. Cyber Defenders Work in Idaho Falls
2012-11-14

Noted cybersecurity expert Alan Paller believes there are only 18 to 20 people in the whole country qualified to protect the nation's infrastructure from a concerted cyber attack. That's an incredibly small number of people considering the hundreds of thousands of engineers working in the private, public and military sectors, but Paller isn't the only person who thinks that's the case.
…
One might expect those superheroes to come from Langley or Palo Alto, but instead, they're more likely to be found in Idaho Falls. Idaho National Labs, the Department of Energy's lead nuclear research and development facility, is also home to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). These are the people companies call for help when they face the most serious of attacks that may have national security implications. The number of incidents that organizations have reported to ICS-CERT has risen to 198 in 2011 from nine in 2009. Team members have traveled on site to help companies on 17 different occasions between 2009 and 2011.
http://blogs.wsj.com/cio/2012/11/14/top-u-s-cyber-defenders-work-in-idaho-falls/

7 elements of a self healing power grid
2012-11-13

Some damage to physical infrastructure is inevitable during severe weather and other disasters, but a smart grid with the ability to anticipate, respond to and isolate damage could mitigate the impact and speed recovery, said Massoud Amin, professor of electrical and computer engineering at the University of Minnesota.

Amin, a senior member of the Institute of Electrical and Electronics Engineers who has been working on the idea of a self-healing grid since 1998, describes it as "a system that uses information, sensing, control and communication technologies to allow it to deal with unforeseen events and minimize their adverse impact."

The current power grid faces serious challenges. The increase in power demand is outstripping capacity, and the deregulation and the fragmentation of the industry means no single company is in charge of the infrastructure within a region, so there is less incentive for investment in upgrades to improve reliability.
http://gcn.com/articles/2012/11/13/7-elements-of-a-self-healing-power-grid.aspx

Could a cyber ecosystem automatically defend government networks?
2012-11-07

Through a recent request for information issued in September, the Homeland Security Department and the National Institute of Standards and Technology are examining the current state of technology and the advances needed to create what they call a healthy and resilient system capable of using a defensive concept called Automated Collective Action. The goal is a broad-based, multi-agency or even global system that could, through machine learning and automated information sharing, detect, mitigate and respond to threats while maintaining mission-critical operations.
http://gcn.com/Articles/2012/11/07/Could-the-Internet-automatically-defend-itself.aspx
https://www fbo.gov/index?id=4557423eee3e1cc840a8c50de0ea306c
http://gcn.com/Articles/2012/11/08/Build-cyber-security-immune-system.aspx
http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
http://gcn.com/articles/2012/11/09/agency-programs-show-outlines-of-future-cyber-ecosystem.aspx

NERC-CIP V5 Encourages Unidirectional Gateways
2012-11-05

The provisionally-approved CIP V5 standards address a wider spectrum of cyber-security technologies than were addressed in previous versions, and in particular the draft V5 standards address and encourage the use of hardware-enforced Unidirectional Security Gateways.

Unidirectional Gateways are a secure alternative to firewalls, and are used in defense-in-depth security architectures for the control systems which operate the power grid. Like firewalls, the gateways integrate control system data sources with business information systems through Electronic Security Perimeters. Unlike firewalls, the gateways cannot introduce security vulnerabilities as a result of this integration. The gateway hardware is "deterministic" - no misconfiguration of any software can cause the gateway hardware to put the safety or the reliability of industrial servers at risk.
http://www.sacbee.com/2012/11/05/4961050/nerc-cip-v5-encourages-unidirectional html

White House orders spy agencies to share cyberthreat intel with companies
2012-10-20

A new White House executive order would direct U.S. spy agencies to share the latest intelligence about cyberthreats with companies operating electric grids, water plants, railroads and other vital industries to help protect them from electronic attacks, according to a copy obtained by The Associated Press.

The seven-page draft order, which is being finalized, takes shape as the Obama administration expresses growing concern that Iran could be the first country to use cyberterrorism against the United States. The military is ready to retaliate if the U.S. is hit by cyberweapons, Defense Secretary Leon Panetta said. But the U.S. also is poorly prepared to prevent such an attack, which could damage or knock out critical services that are part of everyday life.

The White House declined to say when the president will sign the order.
http://www nbcnews.com/technology/technolog/white-house-orders-spy-agencies-share-cyberthreat-intel-companies-1C6578275

State-Sponsored Malware 'Flame' Has Smaller, More Devious Cousin
2012-10-15

Researchers have uncovered new nation-state espionage malware that has ties to two previous espionage tools known as Flame and Gauss, and that appears to be a "high-precision, surgical attack tool" targeting victims in Lebanon, Iran and elsewhere.

Researchers at Kaspersky Lab, who discovered the malware, are calling the new malware miniFlame, although the attackers who designed it called it by two other names – "SPE" and "John." MiniFlame seems to be used to gain control of and obtain increased spying capability over select computers originally infected by the Flame and Gauss spyware.
http://www.wired.com/threatlevel/2012/10/miniflame-espionage-tool/

Gleg releases Ver 1.18 of the SCADA+ Exploit Pack for Immunity Canvas
2012-10-10

On October 10, Gleg released version 1.18 of the SCADA+ Exploit Pack for the Immunity Canvas framework, along with a corresponding version 2.17 of the Agora Exploit Pack.

All of the SCADA exploits included in this release cover 0-day vulnerabilities that have not been previously disclosed, including any published advisories or alerts from ICS-CERT. Two of the systems included in this release do not appear to be high-risk to most critical infrastructure and manufacturing facilities within the USA; however, these products do have references within these industries in other countries so due diligence should be performed

if you own a potentially vulnerable system. A third system, which is actually one of the leading RTOS used by many embedded devices, could pose elevated risk to ICS users.
http://scadahacker.blogspot.com/2012/10/gleg-releases-ver-118-of-scada-exploit.html

Can Science Stop Crime?
2012-10-10

... we meet a genius crime-stopper who has made some terrifying discoveries, including how easy it is for a bad guy to highjack not just your laptop but your kids' toys, medical devices, even your car.
http://www.pbs.org/wgbh/nova/tech/can-science-stop-crime.html

Plot Behind Bank Cyber Attack Thickens; Tools Found in Saudi Arabia
2012-10-05

Security professionals investigating the cyber attacks that crippled the websites of U.S. banks last month have discovered the tools at the heart of the attacks are more complex than previously thought and have also been found in Saudi Arabia.

The findings from security firm Radware (RDWR) suggest the attacks -- which are ongoing -- may be harder to stop than had been hoped.

"If I'm a small band of thugs and I've been using handguns and rifles, I've now given myself electronic access to major weapons systems," said Carl Herberger, vice president of security solutions at Radware.

Herberger said the company has found a variant of the malware in "labs in Saudi Arabia" that is a "slightly different version from what's being used in the wild.
http://www foxbusiness.com/industries/2012/10/05/version-bank-cyber-attack-tools-found-in-saudi-arabia/

In cyberattacks, hacking humans is highly effective way to access systems
2012-09-26

Some went to the Chertoff Group, a national security consulting firm in Washington. Others targeted intelligence contractors, gas pipeline executives and industrial-control security specialists. Each note came with the personal touches of a friend or colleague.

"Attach[ed] is a quote for the Social Media training we discussed," said one message sent on July 3 to the vice president of EnergySec, a federally funded group in Oregon that focuses on the cybersecurity of the nation's power grid.

But like much of the digital universe, the e-mails were not what they seemed. They were cyberweapons, part of a devastating kind of attack known as "social engineering."
http://www.washingtonpost.com/investigations/in-cyberattacks-hacking-humans-is-highly-effective-way-to-access-systems/2012/09/26/2da66866-ddab-11e1-8e43-4a3c4375504a_print html

Release of film: We are Legion: The Story of Hacktivists
2012-09-24

WE ARE LEGION: The Story of the Hacktivists, takes us inside the complex culture and history of Anonymous. The film explores early hacktivist groups like Cult of the Dead Cow and Electronic Disturbance Theater, and then moves to Anonymous' own raucous and unruly beginnings on the website 4Chan. Official release, October 19th.
http://wearelegionthedocumentary.com/about-the-film/

Flawed ORing Networking Devices Expose Oil and Gas Companies to Cyberattacks
2012-09-21

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) owned by the US Department of Homeland Security (DHS) has issued an advisory to warn customers of ORing Industrial Networking devices of a serious vulnerability that exposes their organizations to cyberattacks.

According to ICS-CERT, the security hole was identified by independent security researcher Reid Wightman of Digital Bond. He discovered hard-coded passwords for ORing Industrial DIN-Rail Device Server 5042/5042+ systems.
http://news.softpedia.com/news/Flawed-ORing-Networking-Devices-Expose-Oil-and-Gas-Companies-to-Cyberattacks-293994.shtml

Napolitano: Executive order on cybersecurity is 'close to completion'
2012-09-19

Homeland Security Secretary Janet Napolitano on Wednesday said the cybersecurity executive order that the White House is drafting is "close to completion."
http://thehill.com/blogs/hillicon-valley/technology/250371-napolitano-white-house-draft-cyber-order-qnear-completionq

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

U.S. Official Says Cyberattacks Can Trigger Self-Defense Rule
2012-09-18

Cyberattacks can amount to armed attacks triggering the right of self-defense and are subject to international laws of war, the State Department's top lawyer said Tuesday.
http://www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html

UPCOMING EVENTS

February

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (5 days)
February 11–15, 2013
Idaho Falls, Idaho
Course Description
Registration

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.

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 IN THE FOURTH QUARTER OF 2012

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

- An independent research group composed of Nadia Heninger, J. Alex Halderman, Zakir Durumeric, and Eric Wustrow, ICSA-12-335-01—Post OAK Bluetooth Traffic Systems Insufficient Entropy Vulnerability (2012-11-30)
- Independent researchers Roberto Paleari and Ivan Speziale, ICSA-12-325-01—Sinapsi Devices Multiple Vulnerabilities (2012-11-20)
- Security researcher Celil Unuver of SignalSec LLC and independent researcher Luigi Auriemma, ICSA-12-320-01—ABB AC500 PLC Webserver Buffer Overflow Vulnerability (2012-11-15)
- Independent researcher Dale Peterson of Digital Bond, ICSA-12-271-01 - C3-ilex EOScada Multiple Vulnerabilities (2012-11-01)
- Siemens self-reported, ICSA-12-305-01–Siemens SiPass Server buffer overflow (20121031)
- Independent researcher Reid Wightman of Digital Bond, ICSA-12-297-02–Korenix JetPort 5600 Hard-coded Credentials (2012-10-23)
- Researcher Kuang-Chun Hung of the Security Research and Service Institute-Information and Communication Security Technology Center (ICST), ICSA-12-234-01–GE Intelligent Platforms Proficy Multiple Vulnerabilities (2012-10-15)
- Siemens self-reported, ICSA-12-283-01–Siemens S7-1200 Web Application Cross Site Scripting (2012-10-09)
- Wesley McGrew of Mississippi State University, ICSA-12-283-02–WellinTech KingView User Credentials Not Securely Hashed (2012-10-09)
- Researcher Kuang-Chun Hung of the Security Research and Service Institute-Information and Communication Security Technology Center (ICST), ICSA-12-265-01–Emerson DeltaV Buffer Overflow (2012-09-28)
- Independent researcher Luigi Auriemma, ICSA-12-271-02–Optimalog Optima PLC Multiple Vulnerabilities (2012-09-27)
- Independent researcher Reid Wightman of Digital Bond, ICSA-12-263-02–ORing Industrial Networking IDS-5042 Hard-Coded Credentails Vulnerability (2012-09-19)
- Siemens self-reported, ICSA-12-263-01–Siemens S7-1200 Insecure Storage of HTTPS CA Certificates-ICS-VU-268163–Vulnerability in Siemens PLC (2012-09-19)
- Researcher Daiki Fukumori of Cyber Defense Institute, ICSA-12-262-01–Fultek WinTr SCADA (2012-09-18)
- Siemens self-reported, ICSA-12-256-01–Siemens WinCC WebNavigator Multiple Vulnerabilities (2012-09-12)
- Independent researcher Carlos Mario Penagos Hollmann, ICSA-12-251-01–RealWinDemo dll hijack (2012-09-07)
- ZDI by security researcher Alexander Gavrun, ICSA-12-249-03–Indusoft ISSymbol ActiveX Control Buffer Overflow (9/05/2012)
- Researcher Reid Wightman of Digital Bond, ICSA-12-249-02–WAGO IO 758 Default Linux Credentials (2012-09-05)
- Arbiter Systems self reported, ICSA-12-249-01–Arbiter systems Power Sentinel Denial of Service Vulnerability (2012-09-05)

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2012

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

Daiki Fukumori	Celil Unuver	Reid Wightman
Joel Langill	Knud Erik Højgaard (nSense)	Justin W. Clarke
Rubén Santamarta	Billy Rios	Dan Tentler
Dillon Beresford	Greg MacManus (iSIGHT Partners)	Nadia Heninger
Eireann Leverett	Jake Brodsky	Zakir Duremeric
Secunia	Carlos Mario Penagos Hollmann	Eric Wustrow
Yun Ting Lo (ICST)	Bob Radvanovsky	J. Alex Halderman
Kuang-Chun Hung (ICST)	Adam Hahn	Michael Messner
Terry McCorkle	Manimaran Govindarasu	Wesley McGrew
Shawn Merdinger	Jürgen Bilberger	Cesar Cerrudo

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://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@hq.dhs.gov.