ICS-CERT MONTHLY MONITOR

JULY/AUGUST 2011

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

## CONTENTS



## CYBER TIP

Include an incident preparedness checklist in your security plans and review it regularly. This checklist should include (at a minimum) system documentation such as:

- IP ranges and hostnames
- DNS information
- Software and operating system names, versions, and patch levels
- User and computer roles
- Ingress and egress points between networks
- Essential contact information (ISACs, regulators, law enforcement, ICS-CERT).

**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 Information and Incident Reporting:
http://www.ics-cert.org

# 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.

## INCIDENT RESPONSE—SPEAR PHISHING

### Spear Phishing Incidents Continue to Target Federal and Private Entities

In recent months, ICS-CERT has monitored and responded to an increasing number of spear phishing attacks (targeted emails directed at specific individuals or groups of individuals within an organization) directed at both federal and private industry entities in the energy sector (oil, gas, and electrical) and the nuclear sector. In each case, employees were lured into clicking a link in a specially crafted e-mail that either contained malware or connected to a website that contained malware. Because of the attacks, the facilities were forced to shut down e-mail systems and disconnect from the Internet until the extent of the problem was known and mitigation steps were taken. The reasons for these attacks vary, but are usually attempts to gain access to intellectual property, system designs, corporate strategic planning and financial information, and access to control systems themselves via connected business networks.

Spear phishing attacks require the attacker to use personal or corporate knowledge that would not be considered out of the ordinary by their targets. To gain this knowledge, attackers commonly use social networking sites for quick and easy reconnaissance of information that they need to identify potential targets. Common mistakes that individuals make when using social networking sites include:

- Using weak passwords
- Not enabling privacy settings
- Oversharing information about company activities
- Mixing personal and professional information
- Posting detailed information about relatives or coworkers
- Indiscriminately adding connections on social networking websites
- Clicking on links before verifying their correctness or validity

*(continues on page 2)*

*(continued from page 1)*

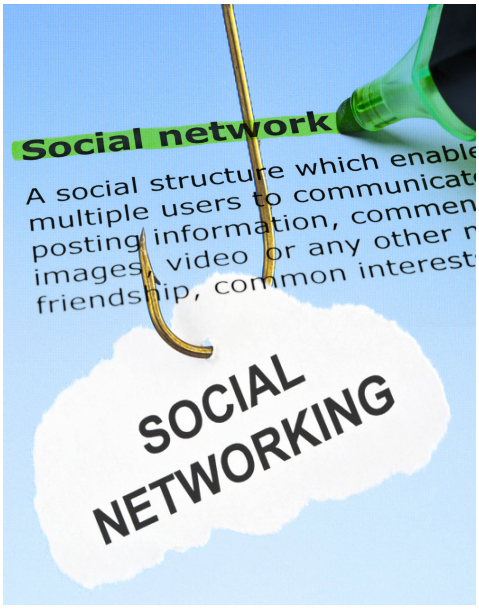
Spear-phishing incidents highlight two important concepts. First, cybersecurity training for all employees is critically important. This includes establishing organizational awareness regarding suspicious e-mails and training on the potential security risks related to personal social networking use. Second, a network layout that employs the recommended defense-in-depth strategies is essential to minimize the potential impact to control systems when an intrusion occurs.

**For more information regarding recognizing and mitigating potential spear-phishing attacks, ICS-CERT recommends the following resources:**

US-CERT, "Staying Safe on Social Network Sites," Cyber Security Tip ST06-003, 2011, http://www.us-cert.gov/cas/tips/ST06-003 html, website last accessed July 27, 2011.

Mindi McDowell, Damon Morda, "Socializing Securely: Using Social Network Services," US-CERT, 2011, http://www.us-cert.gov/reading_room/safe_social_networking.pdf, website last accessed July 27, 2011.

US-CERT, "Cyber Security Tip ST04-014" Avoiding Social Engineering and Phishing Attacks, October 22, 2009, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed July 27, 2011.




## BLACK HAT HIGHLIGHTS

### Black Hat 2011 Highlights

The Black Hat Briefings conference is one of the largest and most anticipated cybersecurity conference series worldwide. This conference consists of the Tool/Demo area for independent security researchers and the open community, the Executive Briefing, Hacker Court, Pwnie Awards, and training. The following list includes control systems related highlights from this year's conference:

- Medical devices—Jerome Radcliffe, a diabetic security analyst demonstrated that manufacturers of pacemakers, insulin pumps, and other medical devices need software defenses to prevent unauthorized manipulation of operating settings, which could potentially turn them off or adjust dosage levels.
- DIY (do it yourself) hacker airborne drone—Mike Tassey and Richard Perkins demonstrated a wireless aerial surveillance platform (WASP), which is designed to fly overhead and sniff/intercept Wi-Fi and cell traffic, or to launch denial of service (DoS) attacks. While the demonstration proved the concept that cellular and Wi-Fi data transmissions are vulnerable to cyber attack, it also demonstrated that this technology could be developed to provide backup critical communications in cases where catastrophic natural events (tsunami, hurricanes, or tornados) have disrupted normal communications. Since many ICS installations use cellular or Wi-Fi technologies for data transmission, the application of this technology should interest critical infrastructure asset owners.
- Siemens PLCs—Dillon Beresford presented on multiple vulnerabilities affecting Siemens S7 PLCs. See the Siemens S7 PLC Support article for more information.

## SIEMENS S7 PLC SUPPORT SUMMARY

Dillon Beresford of NSS Labs has been coordinating with ICS-CERT and Siemens on multiple issues affecting various models within the Siemens SIMATIC Step 7 (S7) programmable logic controller (PLC) product line. His research and public announcements have resulted in seven ICS-CERT Alerts (two limited distribution portal releases and five web releases), and one summary advisory addressing vulnerabilities involving:

1. Use of an open communications protocol
2. Bypass of a password protection mechanism
3. Inadvertent denial-of-service attack putting the PLC into a defective state
4. Access to embedded software within the PLC.

ICS-CERT's summary Advisory titled "ICSA-11-223-01—Siemens SIMATIC S7 PLCs Reported Issues Summary" provides a comprehensive listing of issues, including links to Siemens statements, and recommendations for securing control systems from these and other attack vectors. When evaluating the mitigations available, it is important to recognize that due to the design decisions made in control system industry in the past to foster interoperability, it will not be possible to provide near-term patches for all of the reported issues. In some cases, attempting to retrofit or patch these devices could disrupt the communications required, potentially resulting in a loss of process control. For cases where patching is not possible, some near-term mitigations will be in the form of defense-in-depth practices until long-term architectural changes can be safely adopted, developed, and deployed.

Users of the Siemens SIMATIC S7 product line should consider employing all currently available mitigation strategies. These strategies include a patch developed by Siemens and other defensive measures to harden the automation network environment.

Both ICS-CERT and Siemens take these issues seriously and are working together to prepare a path forward for these and future issues. Please contact ICS-CERT with any questions or comments pertaining to this report.

## ANNOUNCEMENTS

### ICSJWG—ICS Cross-Vendor Position Paper

The increase in ICS vulnerability disclosures and associated media attention has emphasized a new call to arms for a coordinated approach. In 2011 alone, ICS-CERT has seen a 270% increase in reported ICS vulnerabilities affecting multiple systems. Some of the issues involve the use of open protocols and older network architectures that were designed with interoperability in mind, but lack security features that are needed in today's interconnected world. As a result, improving ICS security is not a simple equation and may require extensive architectural changes, including the addition of built-in or layered-on techniques to enhance ICS security.

To address these and other cybersecurity challenges, a task team under the Vendor Subgroup of the Industrial Control Systems Joint Working Group (ICSJWG) was formed. The primary goal is to develop a unified approach for addressing serious security issues that exist across many vendor platforms used in industrial control systems today. The task team will meet regularly to form a strategy for tackling these and other serious security issues facing industrial control systems. The resultant product will be a position paper addressing four main objectives:

1. Document current conditions, challenges, and issues facing asset owners who operate industrial control systems associated with critical infrastructure
2. Outline the barriers to implementing more resilient and secure control system networks as it relates to the open protocol configurations
3. Define an approach that the vendor community can implement to meet the security requirements of owners and operators
4. Develop concepts and plans for implementing change, particularly regarding the addition of security layers to the legacy open protocols, or development of new protocols with built-in security.

The task team is seeking volunteers from

*(announcements continue on page 4)*

## NCCIC NEWS

### DHS' Stempfley and McGurk Testify before the House Committee on Energy and Commerce

Roberta Stempfley, Acting Assistant Secretary of the Office of Cyber Security and Communications, and Seán P. McGurk, Director of the National Cybersecurity and Communications Integration Center (former Director of the Control Systems Security Program and the ICS-CERT), Department of Homeland Security, testified before the United States House of Representatives Committee on Energy and Commerce on July 26, 2011, in response to a request by the House Subcommittee on Oversight and Investigations. The testimony focused on the mission of the department's cybersecurity programs and its ongoing efforts to collaborate with industry and coordinate initiatives to protect critical infrastructure from emerging cyber threats.

To emphasize their concerns, Stempfley and McGurk suggested that, "No single technology—or single government entity—alone can overcome the cybersecurity challenges our nation faces. Consequently, the public and private sectors must work collaboratively. Cybersecurity must start with informed users taking necessary precautions and extend through a coordinated effort among the private sector, including critical infrastructure owners and operators, and the extensive expertise that lies across coordinated government entities." Mr. McGurk also outlined the key aspects of the new National Cybersecurity and Communications Integration Center (NCCIC) and how it is working closely with public and private sector partners to share information and threat awareness data by promoting an atmosphere of teamwork.

The NCCIC encompasses four organizations including the United States Computer Emergency Readiness Team (US-CERT), National Coordinating Center (NCC) for Telecommunications, ICS-CERT, and the DHS Intelligence and Analysis group, which together operate as a team to address emerging cyber threats. This teamwork ranges from intra-agency to international collaboration. To achieve this collaboration, the NCCIC is seeking private industry partners who will work on the NCCIC "watch floor" to share actionable information on a daily basis as new threats emerge. "Together, we can leverage resources, personnel, and skill sets that are needed to achieve a more secure and reliable cyberspace," noted McGurk.

McGurk also commented that, "The Committee was extremely engaging during the hearing and is completely aware of the cybersecurity challenges facing owners and operators of critical infrastructure. They assured us that they are committed to supporting the Department's efforts as we develop and implement solutions with our industry partners."

For a complete transcript of the testimony go to:

http://democrats.energycommerce house.gov/sites/default/files/image_uploads/Testimony_OI_Hearing_07.25.11_StempflyMcgurk.pdf

## ANNOUNCEMENTS

*(continued from page 3*

vendors, owner/operators, and ICS cyber-security subject matter experts to contribute to analysis of these security issues and the development of a documented approach for resolution. Work on the position paper will begin immediately with the development of a scope of work and content outline. For more information or to express interest in participating, please e-mail ICS-CERT at ics-cert@dhs.gov.

### CSSP Rolls Out CSET Version 4.0

The Control Systems Security Program (CSSP) has released Version 4.0 of the Cyber Security Evaluation Tool (CSET). This new version of the tool can be downloaded from the CSSP website http://us-cert.gov/control_systems/satool html. The Version 4.0 release incorporates several new standards, such as NERC CIP Revision 3, NRC Regulatory Guide 5.71, a new key requirements set, and Version 7 of the DHS "Catalog of Security Requirements: Recommendations for Standards Developers." The new CSET tool also includes a fully revised report suite with complete gap rankings, new diagramming functionality, and a new resource library. The updated tool supports evaluations of business and industrial control systems.

### DHS Releases "Private Sector Resources Catalog" (Revision 3)

The Department of Homeland Security (DHS) has released Version 3.0 of the Private Sector Resources Catalog. The Catalog has been completely updated and reorganized to ensure that you and your organization can quickly and easily find all the resources you need. The catalog is targeted specifically towards private sector partners and collects the training, publications, guidance, alerts, newsletters, programs, and services available to the private sector across the entire Department. The Catalog can be downloaded here: http://www.dhs.gov/xabout/gc_1273165166442.shtm

*(announcements continue on page 5*

## ANALYSIS—PRESERVING FORENSIC DATA

### When Suspecting Malicious Activity on Your Network, What Do You Do?

You have the best firewalls configured and managed by a well-trained staff. You have the most recent antivirus system watching e-mail, workstations, and servers. You have managed web proxies configured with good policies. You have a solid network architecture designed from the ground up with security in mind and with an excellent user education program in place, and still you are hacked. Even with the best cyber defense mechanisms in place, you cannot prevent every cyber incident. Are you prepared to properly identify what went wrong and how to recover? A little planning and preparation now will be invaluable when your systems are compromised. To aid asset owners and operators in this preparation, ICS–CERT has identified key elements for developing incident response capabilities necessary to collect data and perform follow-on actions to restore systems to normal operation.

One of the key elements is preserving forensic data. This includes methods for collecting, analyzing, and reporting these data, all of which are important components of any plan to avoid loss of essential information, provide for rapid operational restoration, and improve both near and long-term mitigation and security strategies. The following activities are recommended for preserving these important data in the event of a suspected incident.

- Keep detailed notes of what is observed, including dates/times, mitigation steps taken/not taken, strange or unusual operational behavior, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.
- When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a machine you suspect is compromised from the network.
- Capture forensic images of the system memory and hard drive prior to powering down the system.
- Avoid running any antivirus software "after the fact" as the antivirus scan changes critical file dates, which impedes discovery and analysis of suspected malicious files and timelines.
- Avoid making any changes to the operating system or hardware, including updates and patches, because they will overwrite important information about the suspected malware.

ICS-CERT recommends that organizations consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts as control system environments have special needs that should be evaluated when establishing a cyber forensic plan. For more information regarding control system forensics, ICS-CERT recommends the following resources:

- *Recommended Practice: Creating Cyber Forensics Plans for Control Systems*, Department of Homeland Security, 2008, http://www.us-cert.gov/control_systems/practices/documents/Forensics_RP.pdf.
- *Developing an Industrial Control Systems Cybersecurity Incident Response Capability,* 2009, http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf.
- NIST 800-61, "Computer Security Incident Handling Guide," http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

## ANNOUNCEMENTS

*(continued from page 4*

Monthly Monitor readers will find the chapter titled "Safeguarding and Securing Cyberspace" of particular interest – links provided below:

Full report (62 pages, 2.36 MB)

http://www.dhs.gov/xlibrary/assets/pso-private-sector-resource-catalog-3.pdf

Safeguarding and Securing Cyberspace chapter (4 pages, 417kb)

http://www.dhs.gov/xlibrary/assets/pso-safeguarding-and-securing-cyberspace.pdf

### We Want to Hear from You

A key aspect of our mission is providing cybersecurity products and services to ICS stakeholders. As we develop and prepare new products for our customers, we want your input. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Suggestions for improving our current products are also welcome. Please help us with your feedback as we 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.


## RECENT PRODUCT RELEASES

### ALERTS

**Alert "ICS-ALERT-11-204-01B—(UPDATE) S7-300 Hardcoded Credentials"**

ICS-CERT has updated the original ICS-ALERT as there has been a public release of hardcoded credentials affecting certain older Siemens S7 300 PLCs.

**Alert "ICS-ALERT-11-204-01A—(UPDATE) S7-300_S7-400 Hardcoded Credentials"**

ICS-CERT has updated the original ICS-ALERT as Siemens has determined that the ability to access internal diagnostic functions, as reported by Dillon Beresford, does not affect the S7 400 PLCs and only older, select versions of S7 300 PLCs.

**Alert "ICS-ALERT-11-204-01—S7-300_S7-400 Hardcoded Credentials"**

On July 23, 2011, an independent security researcher publicly announced a vulnerability affecting the Siemens S7 300 and S7 400 PLCs. The researcher claims that he was able to achieve a command shell using credentials he was able to acquire from the PLC.

**Alert "ICS-ALERT-11-186-01—Password Protection Vulnerability in Siemens Simatic Controllers"**

ICS-CERT is continuing to coordinate with Siemens concerning vulnerabilities affecting Siemens SIMATIC Programmable Logic Controllers (PLCs). In May of 2011, security researcher Dillon Beresford of NSS Labs reported multiple vulnerabilities to ICS-CERT that affect the Siemens SIMATIC S7 1200 micro PLC as reported in ICS-CERT ICS-ALERT 11 161 01. The replay attack vulnerabilities affecting the S7 1200 are verified to affect the SIMATIC S7 200, S7 300, and S7 400 PLCs. Siemens PLCs configured with password protection are still susceptible to a replay attack.

**Alert "ICS-ALERT-11-161-01—Siemens S7-1200 PLC"**

ICS-CERT has coordinated with security researcher Dillon Beresford of NSS Labs and Siemens to address multiple vulnerabilities affecting the Siemens SIMATIC S7-1200 micro Programmable Logic Controller (PLC).

### ADVISORIES

**Advisory "ICSA-11-223-01—Siemens SIMATIC PLCs Reported Issues Summary"**

This Advisory provides a summary of the various alerts and notices as well as other public information available to date.

**Advisory "ICSA-11-195-01—Invensys Wonderware Information Server"**

ICS-CERT Advisory ICSA-11-195-01P was released to the US-CERT Portal on July 14, 2011. This web page release was delayed to allow users sufficient time to download and install the update. Independent security researchers Billy Rios and Terry McCorkle have identified a stack-based buffer overflow vulnerability that exists in two different ActiveX controls used by the Wonderware Information Server product. Successful exploitation of this vulnerability could allow remote code execution on a client running vulnerable versions of the software.

**Advisory "ICSA-11-189-01—7-Technologies IGSS Remote Memory Corruption"**

ICS-CERT has become aware of a memory corruption vulnerability that was coordinated with the 7 Technologies (7T) by the VUPEN Vulnerability Research Team. This vulnerability affects the Interactive Graphical SCADA System (IGSS) supervisory control and data acquisition (SCADA) human-machine interface (HMI) application. This vulnerability is remotely exploitable.

## RECENT PRODUCT RELEASES

### ADVISORIES

**Advisory "ICSA-11-182-01—ICONICS TrustedZone Vulnerability"**

ICS-CERT has received a report from independent security researchers Billy Rios and Terry McCorkle concerning ICONICS GENESIS32 and BizViz products. This vulnerability involves a design issue in a GENESIS32 ActiveX control that can set an arbitrary domain to the trusted zone. ICONICS has validated the researchers claims for multiple versions of GENESIS32 and BizViz.

**Advisory "ICSA-11-182-02—ICONICS Login ActiveX Vulnerability"**

ICS-CERT has received a report from independent security researchers Billy Rios and Terry McCorkle concerning a vulnerability that affects ICONICS GENESIS32 and BizViz products. This vulnerability includes a crash in the Security Login controls used by GENESIS32 due to a buffer overflow. ICONICS has validated the researchers' claims for the multiple versions of GENESIS32 and BizViz.

**Advisory "ICSA-11-175-02—Siemens WinCC Exploitable Crashes"**

ICS-CERT Advisory ICSA-11-175-02P was released to the US-CERT Portal on June 24, 2011. This web page release was delayed to allow users sufficient time to download and install the update. ICS-CERT has received a report from independent security researchers Billy Rios and Terry McCorkle concerning exploitable crashes in the Siemens SIMATIC WinCC SCADA product. Specially crafted files can cause memory corruption or pointer issues, which can cause the system to crash.

**Advisory "ICSA-11-168-01A—(UPDATE) InduSoft ISSymbol ActiveX Control Buffer Overflow"**

This is an UPDATE to ICS-CERT Advisory "ICSA-11-168-01—InduSoft ISSymbol ActiveX Control Buffer Overflow" published on June 17, 2011. Security researcher Dmitriy Pletnev of Secunia Research has released details of multiple overflow vulnerabilities affecting the InduSoft ISSymbol ActiveX control.

**Advisory "ICSA-11-122-01—AzeoTech DAQFactory Networking Vulnerabilities"**

This Advisory was previously released on the US-CERT Portal. This web page release was delayed to allow users sufficient time to download and install the update. ICS-CERT received a report from the nSense Vulnerability Coordination Team concerning several vulnerabilities in AzeoTech DAQFactory. Azeotech has created a new version (Version 5.85, Build 1842) to resolve these vulnerabilities.

**Advisory "ICSA-11-175-01—Rockwell FactoryTalk Diag Viewer Memory Corruption"**

Independent researchers Billy Rios and Terry McCorkle have coordinated a memory corruption vulnerability affecting the Rockwell Automation FactoryTalk Diagnostics Viewer product with ICS-CERT.

**Advisory "ICSA-11-168-01—InduSoft ISSymbol ActiveX Control Buffer Overflow"**

Security researcher Dmitriy Pletnevo of Secunia Research has released details of multiple overflow vulnerabilities affecting the InduSoft ISSymbol ActiveX control. The researcher identified both stack-based and heap-based buffer overflows. InduSoft has issued an update addressing this vulnerability.

**Advisory "ICSA-11-167-01—Sunway ForceControl"**

ICS-CERT has received a report from Security researcher Dillon Beresford of NSS Labs concerning heap-based buffer overflow vulnerabilities affecting Sunway ForceControl and pNetPower SCADA/HMI applications. The reported vulnerabilities could result in a denial of service or the execution of arbitrary code.


## UPCOMING EVENTS

### SEPTEMBER

**International Industrial Control Systems Cyber Security Advance Training and workshop (1 week)**

September 12–16, 2011
Control Systems Analysis Center
765 Lindsay Boulevard, Idaho Falls, ID

**The 11th ICS Cyber Security Conference**

Hosted by Applied Control Solutions (ACS)
September 20–22, 2011
Washington Hilton Hotel,
Washington, DC

**The Cyber Security for Energy Delivery Conference**

September 27–28, 2011
Crowne Plaza Hotel, San Jose, CA

### OCTOBER

**NERC GridSecCon 2011**

October 18–20, 2011
JW Marriott, New Orleans, LA

**Industrial Control Systems Joint Working Group (ICSJWG) 2011 Fall Conference**

October 24–27, 2011
Long Beach, CA

### NOVEMBER

**2011 Cyber Security in Transportation Summit**

November 1–2, 2011
Sheraton Crystal City, Arlington, VA

## RECENT PRODUCT RELEASES

### ADVISORIES

**Advisory "ICSA-11-056-01A—(UPDATE) Progea Movicon TCPUploadServe"**

This updated Advisory notifies existing users that known exploits are now targeting this vulnerability.

**Advisory "ICSA-11-161-01—Rockwell RSLinx EDS"**

ICS-CERT has received a report from Michael Orlando of CERT/CC identifying a vulnerability in Rockwell Automation EDS Hardware Installation Tool (RSHWare). This tool is bundled with RSLinx Classic for normal distribution and exhibits a buffer overflow vulnerability when parsing improperly formatted EDS files.

**Advisory "ICSA-11-069-01B—(UPDATE) Samsung Data Management Server"**

This updated website posting provides new information regarding Samsung's process for acquiring the updated software to mitigate the reported vulnerability. José A. Guasch reported a SQL injection vulnerability in the Samsung Data Management Server (DMS).

**Advisory "ICSA-11-132-01A—(UPDATE) 7-Technologies IGSS DoS"**

This Advisory updates the previously released ICS-CERT Advisory titled "ICSA-11-132-01—7-Technologies IGSS Denial of Service." The update provides additional details on affected products, patch validation status, and the download links for patches.

**Advisory "ICSA-11-147-01B—(UPDATE) Ecava IntegraXor DLL Hijacking"**

This updated advisory addresses the possibility of remote exploit execution. It also provides the URL location for the latest patch, which resolves an Uncontrolled Search Path Element vulnerability, commonly referred to as DLL hijacking, in the Ecava IntegraXor supervisory control and data acquisition (SCADA) product.

### COORDINATED VULNERABILITY DISCLOSURE

*ICS-CERT actively works with a variety of researchers and ICS vendors to foster coordinated vulnerability disclosure. The coordinated disclosure process allows time for a vendor to release patches and users to apply patches prior to public disclosure of the vulnerability.*

*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**

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

- nSense – AzeoTech DAQFactory networking vulnerabilities (ICSA-11-122-01)
- Billy Rios and Terry McCorkle – Siemens WinCC exploitable crashes (ICSA-11-175-02)
- Dillon Beresford – Siemens vulnerabilities coordination efforts (ICS-ALERT-11-161-01; ICS-ALERT-11-186-01; ICSA-11-223-01)

**Researchers Currently Working with ICS-CERT**

ICS-CERT appreciates the following researchers who continue to work through the coordinated disclosure process:

| | | |
|---|---|---|
| Ruben Santamarta | Joel Langill | Carlos Mario Penagos Hollmann |
| Morgan Hung | Andrew Lo | Michael Orlando |
| Jeremy Brown | Shawn Merdinger | Knud Hoigaard (nSense) |

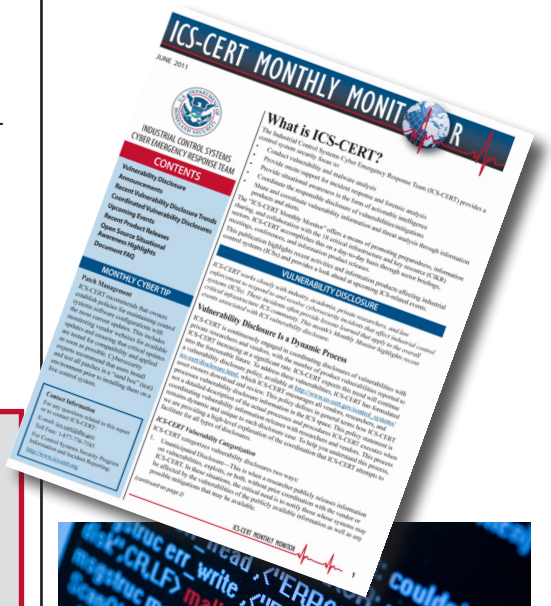
### OTHER

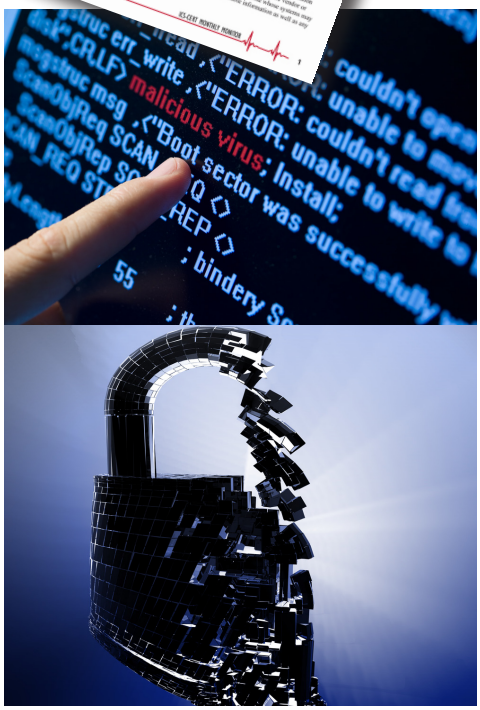
**Announcement-11-208-01—Cross Vendor Working Group**

ICS-CERT is announcing the creation of a Cross Vendor Working Group to work within the ICSJWG toward developing a comprehensive position paper on ICS security.

**The ICS CERT Monthly Monitor for June 2011**

included highlights of activities from May.



## 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.*

### The Pentagon Is Confused About How to Fight a Cyberwar

June 01, 2011

On Tuesday, the Wall Street Journal broke news that the Pentagon decided that cyberattacks [sic] against the United States constitute an act of war and may be answered with the full force of the U.S. military.

http://www.nationaljournal.com/dailyfray/the-pentagon-is-confused-about-how-to-fight-a-cyberwar-20110601

### Defector Claims North Korea Grooms Cyber Terrorists

June 01, 2011

North Korea is expanding its force of future cyber warriors, and is even sending young hacker prodigies abroad to enhance their skills, according to a representative from a group of North Korean defectors, Korea Joongang Daily reports.

http://www.thenewnewinternet.com/2011/06/01/defector-claims-north-korea-grooms-cyber-terrorists/

### List of cyber-weapons developed by Pentagon to streamline computer warfare

June 02, 2011

The Pentagon has developed a list of cyber-weapons and -tools, including viruses that can sabotage an adversary's critical networks, to streamline how the United States engages in computer warfare.

http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html

### Gmail phishers stalked victims for months

June 03, 2011

Spear phishers who targeted the personal Gmail accounts of senior government officials painstakingly monitored incoming and outgoing email for almost a year, a researcher who helped uncover the campaign said.

http://www.theregister.co.uk/2011/06/03/gmail_users_stalked_for_months/

### Hotmail and Yahoo users also victims of targeted attacks

June 03, 2011

Web mail users at Yahoo and Hotmail have been hit with the same kind of targeted attacks that were disclosed earlier this week by Google, according to security software vendor Trend Micro.

http://www.computerworld.com/s/article/9217278/Hotmail_and_Yahoo_users_also_victims_of_targeted_attacks

### Stolen Data Is [sic] Tracked to Hacking at Lockheed

June 03, 2011

Lockheed Martin said Friday that it had proof that hackers breached its network two weeks ago partly by using data stolen from a vendor that supplies coded security tokens to tens of millions of computer users.

http://www nytimes.com/2011/06/04/technology/04security html

### A Utility CEO Who Is Talking About Security

June 04, 2011

Wow! It truly amazes me to hear that the CEO of a large utility is speaking up about the importance of cyber security in the Smart Grid.

http://granitekey.blogspot.com/2011/06/utility-ceo-who-is-talking-about html

### Company SecurID Tokens Will Be Replaced

June 07, 2011

RSA Security, a security data firm that suffered a breach back in March, is now offering to replace all of the security tokens it provides to millions of corporate workers.

http://techland.time.com/2011/06/07/company-securid-tokens-will-be-replaced/

### Hacker to go public with Siemens SCADA control flaws

June 07, 2011

A security researcher who says he's found serious problems with Siemens computers used in power plants and heavy industry is now expecting to go public with his research at the Black Hat security conference.

http://news.techworld.com/security/3284398/hacker-to-go-public-with-siemens-scada-control-flaws/

### To defeat phishing, Energy learns to phish

June 08, 2011

The Energy Department's Oak Ridge National Laboratory received more than 500 e-mails in April that appeared to be from the lab's benefits department and contained a link for more information.

http://gcn.com/articles/2011/06/13/doe-phishing-test.aspx

### Secure the smart grid or face 'serious consequences,' Chu says

June 13, 2011

The administration has released a strategy to help provide unity and coherence to the modernization of the nation's electric power grid.

http://gcn.com/articles/2011/06/13/smart-grid-strategy-security.aspx

### High-profile attacks highlight need for defenses against targeted threats

June 14, 2011

The recent spate of successful cyber attacks against high-profile organizations has focused fresh attention on the need for enterprises to implement new defenses against targeted threats.

http://www.computerworld.com/s/article/9217590/

## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

**National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems (ICS) Security**

June 15, 2011

NIST has published the final version of Special Publication SP800-82 Guide to Industrial Control Systems (ICS) Security.

http://csrc nist.gov/publications/nist-pubs/800-82/SP800-82-final.pdf

**Forget APT, Mass Malware is Still the Big Threat**

June 20, 2011

While the high-profile attacks against RSA, Google and others over the last couple of years has focused a lot of attention on defending against advanced, targeted attacks, the fact remains that most attackers are in fact relying on crimeware packs loaded with commodity exploits for older vulnerabilities that have no trouble bypassing the security systems deployed at the vast majority of enterprises today.

http://threatpost.com/en_us/blogs/forget-apt-mass-malware-still-big-threat-062011

**US experts publish top 25 computer security vulnerabilities**

June 28, 2011

The Department of Homeland Security, in conjunction with the SANS Institute and Mitre, has published a list of this year's top 25 security vulnerabilities, and released new tools for measuring software security risks.

http://www.v3.co.uk/v3-uk/news/2082012/dhs-sans-institute-mitre-publish-security-vulnerabilities

**Symantec's Healthcare Expert: Substantial Risk for Cyber Attack on Medical Devices**

June 28, 2011

Although there has not yet been a planned cyber attack on medical devices, the "collateral damage" of viruses has infected the medical community, according to Axel Wirth, healthcare solutions architect at Symantec.

http://www.thenewnewinternet.com/2011/06/28/symantecs-healthcare-expert-substantial-risk-for-cyber-attack-on-medical-devices/

**The 25 most dangerous programming errors**

June 28, 2011

A coalition of government, academic and private sector security organizations on June 27 released an updated version of the list of the top 25 coding errors considered to be responsible for the majority of security vulnerabilities plaguing software.

http://gcn.com/articles/2011/06/28/cwe-top-25-programming-errors.aspx

**Tests Show Wireless Network Could Harm GPS Systems**

June 30, 2011

Test results filed with federal regulators Thursday show that a proposed high-speed wireless broadband network being planned by a Virginia company called LightSquared could interfere with GPS systems used for everything from aviation to high-precision timing networks to consumer navigation devices.

http://abcnews.go.com/Technology/wireStory?id=13966831

**Two weeks after breach, Energy lab back online**

July 15, 2011

Almost two weeks after an Advanced Persistent Threat forced the Energy Department's Pacific Northwest National Laboratory in Richland, Wash.

http://gcn.com/articles/2011/07/15/pnnl-back-online-after-hack.aspx

**Fixing The Internet May Mean Building A New One**

July 15, 2011

As hackers expose widespread cybersecurity lapses and heighten fears about defending critical infrastructure from attack, one proposed solution has started gaining traction: Rather than attempt to tighten security on the modern Internet, it suggests creating an entirely new one.

http://www huffingtonpost.com/2011/07/15/cyber-security-network-private-internet_n_899364.html

**Embedded Web Servers Exposing Organizations To Attack**

July 21, 2011

"A researcher who has been scanning the Internet for months looking for unsecured, embedded Web servers has found a bounty of digital scanners, office printers, VoIP systems, storage devices, and other equipment fully exposed and ripe for attack.

http://www.darkreading.com/taxonomy/index/printarticle/id/231002364

**'War Texting' Attack Hacks Car Alarm System**

July 25, 2011

Researcher will demonstrate at Black Hat USA next week how 'horrifyingly' easy it is to disarm a car alarm system and control other GSM and cell-connected devices.

http://www.darkreading.com/security/news/231002602/


## DOCUMENT FAQ

**What is the publication schedule for this digest?**

ICS-CERT publishes the "ICS-CERT Monthly Monitor" approximately 12 times per year. With the exception of this two-month issue, 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