ICS-CERT MONTHLY MONITOR

January 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

NOTEWORTHY INCIDENTS IN DECEMBER

SITUATIONAL AWARENESS

ANNOUNCEMENTS

UPCOMING EVENTS

NCCIC NEWS

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

SECTOR SECTION

COORDINATED VULNERABILITY DISCLOSURE

Contact Information

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

E-mail: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

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

http://www.ics-cert.org

NOTEWORTHY INCIDENTS IN DECEMBER

Chemical Sector

Recently, ICS-CERT responded to a reported cyber incident at a US chemical company. The company reported the presence of an infection in their business network and they suspected that data had been exfiltrated. In response to the initial report, ICS-CERT provided extensive analytical support to the company, including analysis of file system images, memory dumps, firewall logs, and malware samples.

At the request of the company, ICS-CERT deployed an on-site fly away team to work directly with company personnel to conduct further analysis and gather additional data to further the investigation of the incident. ICS-CERT analysis confirmed the presence advance persistent malware and sophisticated techniques to maintain presence. Interestingly, the malware did not appear to propagate opportunistically like traditional malware, an indication that it was possibly more directed in choosing its victim hosts.

ICS-CERT assisted the company with identifying the scope of the infection and by providing analysis and mitigations for eradicating the threat actor from their network. Asset owners and operators should consider the value of their Intellectual Property (IP) and use defense in depth strategies to protect their networks and data.

Transportation Sector

In early December, 2011, ICS-CERT responded to a cybersecurity incident affecting a rail company. The initial report indicated that the rail company was experiencing a cyber attack to its secondary communications equipment.

ICS-CERT, working in coordination with US-CERT and the asset owner, analyzed various data and determined that the incident was not the result of a targeted attack. In this case, the rail company quickly implemented effective measures to maintain the safety of its operation and worked closely with ICS-CERT to understand the incident and take appropriate mitigating measures. ICS-CERT made the following determinations:

- Redundant communications equipment at the switchgear received erroneous SNMP traffic with spoofed source IP addresses causing intermittent loss of secondary/back-up communications.
- Primary communications were unaffected.
- Control of rail assets by the asset owner were maintained throughout the course of the incident.
- Defense-in-depth cybersecurity measures and ensuring that devices were not Internet facing would have prevented the incident from occurring.

ICS-CERT worked with the company and made specific recommendations for implementing these countermeasures.

ICS-CERT also worked with the Transportation ISAC to issue information to the transportation sector to warn of the activity as it was occurring. ICS-CERT has no indications or reports that any other operators experienced similar activity.

This incident underscores that Critical Infrastructure Key Resource (CIKR) owners and operators should evaluate existing cybersecurity countermeasures they have in place against broader cybersecurity risks. Any number of non-targeted cybersecurity events can impact operations when systems are Internet accessible.

About ICS-CERT Incident Response: ICS-CERT conducts a variety of incident response activities in order to assist asset owners and operators when malicious activity is suspected. These incident response activities include both on-site fly away and offsite technical analysis. More information about ICS-CERT incident handling can be found in our Incident Handling Brochure.

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

Industrial Cellular Security

The use of cellular technologies within industrial control systems (ICSs) offers function and flexibility when competing communication services do not exist or are more costly. Cellular devices are often deployed in remote areas to communicate control functions and alarm reporting. A variety of cellular devices are available for industrial control applications, including the following:

- **Cellular routers**[a,b]—connect remote Ethernet devices to a cellular network, providing network protocol routing.
- **Cellular IP gateways**—process outgoing TCP/IP connections. When configured for network address translation (NAT), a gateway can connect multiple devices to a single service provider IP address. This allows a subnet of internal IP addresses to connect to a single outgoing IP address, thus enabling connections to remote servers.

  Many industrial cellular gateways offer few security features, which create challenges for securing wireless networks. Cellular gateways transmit radio frequencies that can be intercepted in the airways or in the service provider network. They generally do not offer encryption or support firewalls.
- **Cellular IP modems**—connect serial devices to a cellular network. Cellular modems can be fully integrated into a device, an optional adapter board, or an external device connecting directly to a serial port. Many product vendors do not offer security features at the modem level.

  Cellular modems typically provide no security features. Cell modems transmit the serial input data directly to the receiver without security. However, some ICS vendors now offer serial data cryptographic transceivers that can be installed between the end device and the modem to provide advanced cryptographic encryption and security.

Cellular service providers share responsibility for overall system security as it involves more than the owner's industrial control networks. Therefore, cellular service providers should be included in periodic security audits and regular discussions regarding efforts to improve cellular network security.

Mitigation for ICS Cellular Device Threats

Below are general mitigation recommendations for any of the previously mentioned devices.

- If the device has a firewall, turn it on. It's a critical line of defense. And ensure that logging is enabled. Test and audit firewall rules regularly to see how well they are working and confirm they've not had unauthorized changes.
- If the device supports a user name and password, change the default user name and password before installation. If the device is already installed, immediately change the default user name and password. Use strong passwords of 8 to 12 characters mixing extended ASCII characters, numbers, and letters (changing case) as possible for the device. Many device installation manuals and other documentation are readily available on the Internet and frequently contain default user names and passwords, making the device a serious security risk if the default credentials are not changed prior to installation.
- If a device only provides local password management, log in regularly and change the password.
- If the device supports encryption, enable it. If the device supports multiple encryption technologies, use the strongest encryption the network devices support. Even if the strongest encryption technology is not supported by all network devices, some encryption is better than no encryption, provided that system response time is not unacceptably affected.
- Regularly upgrade device firmware with vendor patches. These often provide valuable fixes for identified vulnerabilities.
- Back up configuration files and settings. If the device does not support backups, take screen shots and save them for auditing and future recovery needs.
- Include cellular devices in regular network security audits to validate configuration settings, and when re-evaluating and testing network security based on current and emerging cyber threats.
- Evaluate cellular devices that have limited or no security features for replacement by devices offering secure communication capabilities.

In addition to the general recommendations above, the following specific mitigations should be considered.

- **Cellular routers**—limit the use of port forwarding. If port forwarding is needed, use manual port forwarding and do not rely on Universal Plug 'n' Play (UPnP). Routers can be vulnerable to JavaScript exploits via browsers, enabling rogue websites to alter router settings. This also applies to installed applications. Disabling UPnP prevents accidents when mitigating by using secure browsers, antivirus, etc., and allows greater user control over the network. For generally static ICS environments, port forwarding is manageable and can prevent potential mistakes.
- **Cellular gateways**—any device connected to a gateway Ethernet port should have routing capabilities enabled for security. If a device does not support security, locate a router between the cellular gateway and end devices to provide routing and logging capability. This allows data traffic limiting and port traffic auditing.
- **Cellular modems**—enable all available security features that the modem supports, but do not rely on cellular modems for comprehensive network security.

a. Vanessa Antoine, et al., "Router Security Guidance Activity of the Systems and Network Attack Center (SNAC)," National Security Agency, December 15, 2005, http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf, last accessed December 15, 2011.

b. Dedoimedo, "Router Security," http://www.dedoimedo.com/computers/router_security.html, last accessed December 15, 2011.

ANNOUNCEMENTS

Control Systems Security Program (CSSP) Wins Cybersecurity Innovation Award

The SANS has announced that the DHS National Cyber Security Division supported by the Idaho National Laboratory has won the 2011 U.S. National Cybersecurity Innovation Award for building cybersecurity skills needed to defend major elements of the nation's critical infrastructure sectors. The DHS CSSP offers a range of teaching and educational programs ranging from basic skills to specialty-tailored events to teach, train, and exercise both offensive and defensive cybersecurity skills with the primary purpose to sharpen and expose attendees to possible cyber attack vectors. The goal is to improve awareness and effective self-testing cybersecurity testing, reducing risks across all critical infrastructure and key resource sectors. Training programs have been tailored to federal, state, local, tribal governments, industrial control system owners, integrators, and vendors using control systems.

http://www.homelandsecuritynewswire.com/dr20111228-dhs-idaho-lab-win-cyber-security-innovation-award.

CSSP Releases Version 4.0.1 of the Cyber Security Evaluation Tool (CSET)

CSSP has released Version 4.0.1 of the CSETTM. This new version of the tool can be downloaded. This new release includes 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 CSETTM also includes a fully revised set of reports with complete gap rankings, new diagramming functionality, and a new resource library as well as minor enhancements. This tool supports evaluations of both business and industrial control systems.

CSSP Announces the ICSJWG 2012 Spring Conference – Savannah, GA May 7−10, 2012

The Industrial Control Systems Joint Working Group (ICSJWG) 2012 Spring Conference will be held on May 7−10, 2012, in Savannah, Georgia, USA at the Hyatt Regency Savannah. This event will provide an opportunity for control systems stakeholders from industry, government, academia, international, vendor, and research and development communities to network and engage in discussions related to securing control systems.

The ICSJWG Conference will consist of panel discussions, presentations, training, and working group meetings on various topics such as responsible disclosure, standards development, threat and incident reporting, analysis tools and techniques, roadmap development initiatives, vulnerability management, research and development, and information sharing.

An 8-hour Introduction to Control Systems Cybersecurity training course will also be offered on Thursday, May 10, 2012, at the conference site. Attendance at the conference is not required to attend the training.

The registration site is still being developed. Information about the ICSJWG 2012 Spring Conference can be found at:

http://www.us-cert.gov/control_systems/icsjwg/conference.html.

UPCOMING EVENTS

FEBRUARY

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)

February 13–17, 2011

Control Systems Analysis Center

Idaho Falls, Idaho

Course Description

Registration

MARCH

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)

March 12–16, 2012

Control Systems Analysis Center

Idaho Falls, Idaho

Course Description

Registration

Photo courtesy of the SANS Institute

Left to right: Ken Rohde and Rita Wells of the Idaho National Laboratory and Neil Hershfield of the Department of Homeland Security jointly receive the 2011 National Cybersecurity Innovation Award from White House Cyber Security Coordinator, Howard Schmidt at the National Cybersecurity Innovation Conference in Washington DC.

Control Systems Security Program/ICS-CERT—2011 Highlights

The Department of Homeland Security's Control Systems Security Program (CSSP) recently published a "Year- in-Review" detailing 2011 program highlights for ICS-CERT as well as other CSSP program areas. Other areas include the Industrial Control Systems Joint Working Group efforts, cybersecurity assessments, training, and roadmaps and standards initiatives.

The following snapshot provides some insight into the broader scope of important CSSP initiatives and milestones for last year.

Industrial Control Systems Joint Working Group (ICSJWG)

Approximately 600 participants from the public and private sector attended the Fall 2010 and Spring 2011 ICSJWG Conferences, with over 200 attending the Fall 2011 ICSJWG Conference.

In 2011, the Working Group finalized the Cross-Sector ICS Cybersecurity Roadmap, which addresses a broad range of cybersecurity strategies relevant to sectors that may not have completed their own roadmaps.

CSET and CSET Assessments

CSSP released V4 of the Cyber Evaluation Tool (CSET™) in August. Over 1,150 CSET™ copies were distributed in FY 2011, and CSSP has now made the tool downloadable from the website (http://www.us-cert.gov/control_systems/satool.html - Version 4.0.1 is now available).

CSSP also supported over 75 CSET onsite assessments, across multiple sectors, with CSSP staff working directly with asset owners to train them in the use of the tool. The onsite assessments are conducted at no cost to the asset owners.

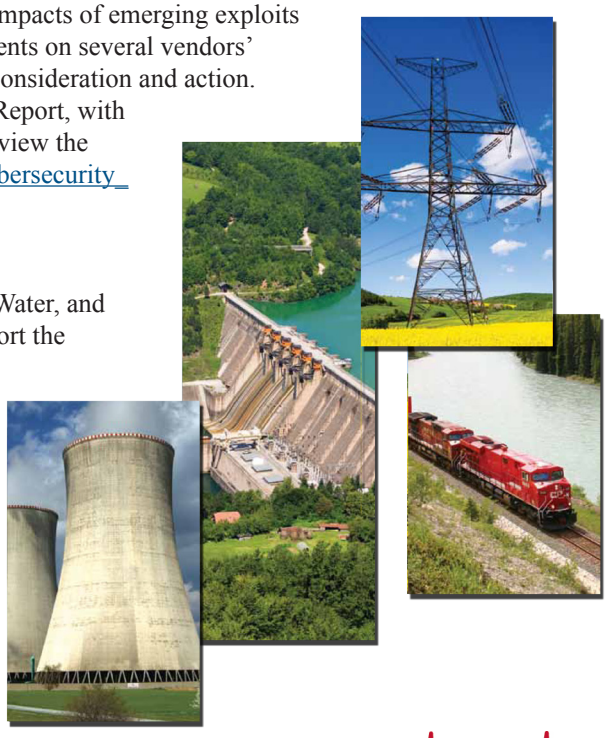
Cybersecurity Training

In 2011, CSSP provided over 40 training courses domestically and internationally – frequently held in conjunction with cybersecurity conferences – for public and private partners. Over 1,300 persons attended CSSP training in 2011. Training courses include Introductory, Intermediate, and Advanced ICS classes. The week-long Advanced ICS class is a hands-on course that culminates in a Red-Blue exercise in an actual control system environment. All the training courses are provided free of cost to participants.

In April 2011, CSSP also released a new Management Level Training Course to provide a high-level overview of ICS security for managers. To find out more about CSSP training events, visit http://www.us-cert.gov/control_systems/cstraining.html#workshop.

Vendor Assessments

CSSP vendor assessments focus on identifying vulnerabilities and potential impacts of emerging exploits in specific vendor equipment or software. In 2011, CSSP completed assessments on several vendors' systems and provided findings and recommendations to system vendors for consideration and action. This information also feeds into the Common Cybersecurity Vulnerabilities Report, with the most recent one published in May of 2011. For more information or to review the report, visit http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf.



Roadmaps and Standards

CSSP supports roadmap development efforts in the Dams, Energy, Nuclear, Water, and Transportation sectors through various partnerships. CSSP continues to support the efforts of standards organizations to develop new cybersecurity standards and to advance existing efforts. Some areas in which CSSP is involved include Smart Grid Interoperability Panel (SGIP), the SGIP Cybersecurity Working Group, ISA-99, and the APTA Cyber Security Recommended Practices.

Conclusion

For more details on CSSP 2011 activities, please follow this link to the "CSSP Year-in-Review."

ICS-CERT will publish a separate "ICS-CERT Annual Review" in February 2012 (www.ics-cert.org).

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-11-343-01 - Control Systems Internet Accessibility"

On October 28, 2010, ICS-CERT published an alert titled "ICS-ALERT-10-301-01 - Control System Internet Accessibility" on the ICS-CERT web page. The alert warned control system owners and operators that a search engine called SHODAN was being used to locate Internet facing control systems. ICS-CERT is issuing this new alert to warn of an uptick in related activity and urge asset owners and operators to audit their control systems configurations and verify whether they are susceptible to an attack via this vector.

ICS-CERT is tracking and has responded to multiple reports of researchers using SHODAN, Every Routable IP Project (ERIPP), Google, and other search engines to discover Internet facing control systems. ICS-CERT has coordinated this information with the identified control system owners and operators to notify them of their potential vulnerability to cyber intrusion and attack. When appropriate, ICS-CERT also coordinates with the corresponding sector Information Sharing and Analysis Centers (ISACs) or international CERT/CIRT to notify asset owners. In many instances, the exposed systems were unknowingly or unintentionally configured with potentially unsecure access authentication and authorization mechanisms. ICS-CERT works with the asset owner/operators and vendor or systems integrators whenever possible to remove any default credentials and secure these systems from attack.

In cases where unauthorized access has been identified, ICS-CERT has assisted control system owners and operators with system and firewall data analysis to determine the extent of the intrusion and whether any configuration changes might have been made to the system.

The use of readily available and generally free search tools significantly reduces time and resources required to identify Internet facing control systems. In turn, hackers can use these tools to easily identify exposed control systems, posing an increased risk of attack. Conversely, owners and operators can also use these same tools to audit their assets for unsecured Internet facing devices.

Alert "ICS-ALERT-11-336-01A - 3S CoDeSys Multiple Vulnerabilities"

ICS-CERT is aware of additional public reporting of vulnerabilities with PoC exploit code affecting 3S CoDeSys web server. This report includes the buffer overflow previously reported, as well as three additional vulnerabilities. This report was released by Luigi Auriemma without coordination by ICS-CERT, the vendor, or any other coordination entity of which ICS-CERT is aware.

ICS-CERT is issuing this updated alert to provide notice of the additional report vulnerabilities and to identify baseline mitigations for reducing risks to this and other cybersecurity attacks.

The reports include vulnerability details and PoC exploit code for the following vulnerabilities

Alert "ICS-ALERT-11-336-01 - 3S CoDeSys Webserver Buffer Overflow"

ICS-CERT is aware of a public report of Buffer Overflow vulnerability with proof-of-concept (PoC) exploit code affecting 3S CoDeSys web server, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, the vulnerability is exploitable by sending specially crafted packets to the server Port 8080/TCP. This report was released by Celil Unuver of SignalSEC Labs.

ICS-CERT has reached out to the affected vendor to notify, confirm, and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

Alert "ICS-ALERT-11-332-02A - Siemens SIMATIC WinCC Flexible"

This Alert Update is a follow-up to the original ICS-CERT Alert titled "ICS-ALERT-11-332-02A - Siemens SIMATIC WinCC Flexible Vulnerabilities" that was published November 28, 2011 on the ICS-CERT web page.

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting WinCC Flexible Runtime Loader, a component of Siemens SIMATIC WinCC Flexible 2008. When the Runtime Loader is running in Transfer mode, it may be possible to remotely exploit the vulnerabilities via Port 2308/TCP. This report was released by Luigi Auriemma without coordination with ICS-CERT, the vendor, or other coordination entity of which ICS-CERT is aware.

ICS-CERT has coordinated the report with Siemens, who is working to confirm the report and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

Alert "ICS-ALERT-11-332-01A - Siemens Automation License Manager"

This Alert Update is a follow-up to the original ICS-CERT Alert titled "ICS-ALERT-11-332-01-Siemens Automatic License Manager" that was published November 28, 2011, on the ICS-CERT web page.

ICS-CERT is aware of a public report of four vulnerabilities with proof-of-concept (PoC) exploit code affecting the Siemens Automation License Manager (ALM). According to this report, the vulnerabilities are remotely exploitable. This report was released by Luigi Auriemma without coordination with Siemens, ICS-CERT, or any other coordinating entity known to ICS-CERT.

ICS-CERT has coordinated the report with Siemens, who is working to confirm the report and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The ALM is a component of Siemens industrial software and is necessary for licensing Siemens supervisory control and data acquisition (SCADA), human-machine interface (HMI), and engineering software.

The report includes vulnerability details and PoC exploit code for four vulnerabilities. Siemens has analyzed the vulnerability report and offered the following vulnerability characterization information.

RECENT PRODUCT RELEASES

ADVISORIES

Advisory "ICSA-11-362-01 - ScadaTEC ScadaPhone and ModBusTagServer Buffer Overflow"

This advisory is a follow-up to the ICS-CERT alert titled "ICS-ALERT-11-255-01 - ScadaTEC ScadaPhone/ModbusTag-Server Buffer Overflow" that was published September 12, 2011, on the ICS-CERT web page.

On September 12, 2011, independent security researcher Steven Seeley publicly released a report that included proof-of-concept (PoC) exploit code targeting a buffer overflow vulnerability in the ScadaTEC ScadaPhone and ModbusTagServer products. Currently, the exploit code allows an attacker to bind a shell for remote access.

According to the report, exploitation of this vulnerability requires a specially crafted ZIP file to be opened using the affected application.

ScadaTEC has produced a patch that resolves this vulnerability for all affected products and versions. ICS-CERT has validated that these patches fully resolve the vulnerability.

Advisory "ICSA-11-361-01 - Siemens Automation License Manager"

This Advisory is a follow-up to the original Alert titled "ICS-ALERT-11-332-01A - Siemens Automation License Manager Multiple vulnerabilities" that was published December 02, 2011, on the ICS-CERT web page.

ICS-CERT is aware of publicly disclosed reports of four vulnerabilities in Siemens Automation License Manager (ALM) application. These vulnerabilities include:

- Buffer overflow
- Exception
- Null pointer
- Improper input validation.

Independent researcher Luigi Auriemma publicly disclosed four vulnerabilities along with proof-of-concept (PoC) exploit code without coordination from Siemens, ICS-CERT, or any other coordinating entity known to ICS-CERT.

Siemens has confirmed these vulnerabilities and has released a patch to address the issue. ICS-CERT has not validated the patch.

Advisory "ICSA-11-356-01 - Siemens Simatic HMI AuthenticationVulnerabilities"

ICS-CERT is aware of a public report by independent security researchers Billy Rios and Terry McCorkle concerning authentication bypass vulnerabilities affecting Siemens SIMATIC HMI products, which are supervisory control and data acquisition/human-machine interface (SCADA/HMI) products.

According to this report, systems running affected versions of this product are accessible using a default username and password. These systems also generate an insecure authentication token for browser sessions. Prior to public disclosure, the researchers notified ICS-CERT of the vulnerabilities. ICS-CERT is continuing to coordinate mitigations with the researchers and Siemens.

Siemens was previously aware of these vulnerabilities and intends to address them in Service Packs to be released in January 2012. Please see mitigation section of this document for additional information regarding the release of the Service Packs. Siemens has also updated its product documentation with instructions for configuring a strong password and removing default passwords during initial setup.

Advisory "ICSA-11-355-02 - WellinTech KingView History Server Buffer Overflow"

ICS-CERT has received a report from the Zero Day Initiative (ZDI) concerning a heap-based buffer overflow vulnerability in WellinTech Kingview HistoryServer.exe, which may allow a remote, unauthenticated attacker to execute arbitrary code. This vulnerability was reported to ZDI by independent security researcher Luigi Auriemma.

WellinTech has produced a patch that is available for download from its website.

Advisory "ICSA-11-355-01 - 7-Technologies IGSS Buffer Overflow"

Security researcher Celil Unuver ICS-CERT has has identified a buffer overflow vulnerability in the 7-Technologies (7T) Interactive Graphical SCADA System (IGSS) product. Successful exploitation of this vulnerability could result in a denial of service (DoS) or the execution of arbitrary code. ICS-CERT has coordinated this vulnerability report with 7T, and they have produced a patch that resolves this vulnerability. The researcher has confirmed that the patch fully resolves the reported vulnerability.

Advisory "ICSA-11-335-01 - 7-Technologies Data Server Buffer Overflow"

ICS-CERT originally released advisory ICSA-11-335-01P - 7-Technologies Data Server Denial of Service in the US CERT secure portal on December 01, 2011. This web page release was delayed to allow users time to download and install the update.

Security researcher UCQ from the Cyber Defense Institute, Inc. has identified a buffer overflow vulnerability in the 7 Technologies (7T) IGSS Data Server application.

ICS-CERT has coordinated with 7T, which has produced a patch to resolve this vulnerability. The Cyber Defense Institute, Inc. has tested the patch and confirmed that it resolves the reported vulnerability.

Advisory "ICSA-11-314-01 - Safenet Sentinel and 7-T Input Sanitization Vulnerability"

ICS-CERT originally released advisory ICSA-11-314-01P on the US-CERT secure portal on November 14, 2011. This web page release was delayed to allow users time to download and install the update.

Security researcher Carlos Mario Penagos Hollman of Synapse-labs has identified an input sanitization vulnerability in SafeNet Sentinel HASP Software Rights Management (HASP-SRM) license management application.

ICS-CERT has coordinated the researchers vulnerability report with SafeNet, and SafeNet has produced an updated version that mitigates this vulnerability. Mr. Penagos has tested the updated version and validates that it resolves the vulnerability.

RECENT PRODUCT RELEASES

Advisory "ICSA-11-298-01A—Sielco Systemi Winlog Buffer Overflow Update A"

Update A adds the following text in the section titled "Mitigation": Sielco Systemi advises users to download the new Winlog release, from their website www.sielcosistemi.com and follow download instructions found there.

Advisory "ICSA-11-298-01 - Sielco Systemi Winlog Buffer Overflow"

ICS-CERT originally released Advisory ICSA-11-298-01P on the US-CERT secure portal on October 25, 2011. This web page release was delayed to allow users time to download and install the update.

Independent researcher Paul Davis has identified a buffer overflow vulnerability in Sielco Systemi Winlog application. Sielco Systemi has produced a new release that mitigates this vulnerability. Mr. Davis has indicated to ICS-CERT that he has tested the new release and validated that it resolves the vulnerability

Advisory "ICSA-11-340-01 ARC Informatique PcVue Multiple Vulnerabilities"

This Advisory is a follow-up to the Alert, "ICS-ALERT-11-271-01-PcVue HMI/ SCADA Multiple ActiveX Vulnerabilities" that was published September 28, 2011, on the ICS-CERT web page.

ICS-CERT is aware of publicly and privately disclosed reports of four vulnerabilities in ARC Informatique's PcVue application. These vulnerabilities include denial of service, potential to write memory, possible file corruption, and remote code execution.

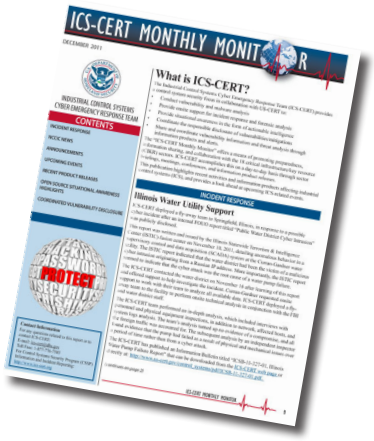
Independent researcher Kuang-Chun Hung of Security Research and Service Institute Information and Communication Security Technology Center (ICST) privately identified a buffer overflow vulnerability in ARC Informatique's PcVue application.

Independent researcher Luigi Auriemma publicly disclosed four vulnerabilities along with proof-of-concept (PoC) exploit code, including the vulnerability privately disclosed by ICST, without coordination with Siemens, ICS-CERT, or any other coordinating entity of which ICS-CERT is aware.

ARC Informatique has confirmed this vulnerability and has released a patch to address the issue. Researcher Kuang-Chun Hung has tested the patch and validated that it resolves these vulnerabilities.

OTHER

The ICS CERT Monthly Monitor December 2011 issue includes highlights of activities from November 2011.



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.

DOCUMENT FAQ

What is the publication schedule for this digest?

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

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT web page at: http://www.us-cert.gov/control_systems/ics-cert/.

Please direct all questions or comments about the content, or suggestions for future content, to ICS-CERT at

ics cert@dhs.gov

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.

Lethal Stuxnet cyber weapon is 'just one of five' engineered in same lab - and three have not been released yet

December 29, 2011

- Cyber weapons designed to attack industrial plants
- Software 'seeks out' other members of same family
- Three 'missing' members have not been used yet
- Designed in lab over last four years - probably by U.

http://www.dailymail.co.uk/sciencetech/article-2079725/Lethal-Stuxnet-cyber-weapon-just-engineered-lab.html

Stuxnet/Duqu: The Evolution of Drivers

December 28, 2011

"We have been studying the Duqu Trojan for two months now, exploring how it emerged, where it was distributed and how it operates. Despite the large volume of data obtained (most of which has yet to be published), we still lack the answer to the fundamental question - who is behind Duqu?"

https://www.securelist.com/en/analysis/204792208/Stuxnet_Duqu_The_Evolution_of_Drivers

Embedded attacks and emerging targets to dominate 2012 security landscape

December 28, 2011

"McAfee has painted a gloomy security picture for 2012 in which enterprises and criminals shift to new platforms and tactics for securing and infiltrating networks."

http://www.v3.co.uk/v3-uk/news/2134518/embedded-attacks-emerging-targets-dominate-2012-security-landscape

Cyber Threat to Power Grid Puts Utility Investors at Risk

December 27, 2011

"The electric-utility industry's concerns about cyber security has escalated sufficiently for several investor-owned utilities to include cyber-attacks as a material risk factor in recent filings with the U."

http://www.forbes.com/sites/williampentland/2011/12/27/cyber-threat-to-power-grid-puts-utility-investors-at-risk/

Homeland Security Warns SCADA Operators Of Internet-Facing Systems

December 12, 2011

"In the wake of the hack of water and sewer infrastructure operated by a Texas community, the Department of Homeland Security is again warning owners and operators of critical infrastructure to take note of SCADA and industrial control systems that may be accessible from the Internet."

http://threatpost.com/en_us/blogs/homeland-security-warns-scada-operators-internet-facing-systems-121211

Cyber attacks could wreck world oil supply

December 08, 2011

(Reuters) – "Hackers are bombarding the world's computer controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil supply disruption."

http://www.reuters.com/article/2011/12/08/us-cyber-attacks-oil-idUSTRE7B71FI20111208?feedName=technologyNews&feedType=RSS

Potash hackers a wake-up call for lawyers

Dec 06, 2011

"Reports last week revealed that computer hackers in China who had "attacked" the federal Department of Finance, Treasury Board and departments within the Saskatchewan government in 2010 were attempting to obtain confidential information about the $40 billion takeover attempt of Potash Corp. of Saskatchewan by Australian company BHP Billiton Ltd., a sale Ottawa refused to approve."

http://www.theglobeandmail.com/report-on-business/small-business/sb-growth/day-to-day/potash-hackers-a-wake-up-call-for-lawyers/article2261700/

Duqu attackers: master coders, Linux rookies

December 01, 2011

"Amateur goofs doom global wipe of C&C servers."

http://www.theregister.co.uk/2011/12/01/duqu_linux_goofs/

SECTOR SECTION

Chemical Facility Anti-terrorist Standards (CFATS)

Section 550 of the 2007 Department of Homeland Security (DHS) appropriations bill (P.L. 109 295)(Act), provided DHS with regulatory authority over security at high-risk chemical facilities. This act requires all high-risk chemical facilities to complete security vulnerability assessments (SVA), develop site security plans (SSP), and implement protective measures necessary to meet 18 DHS-defined risk-based performance standards (RBPS). High-risk chemical facilities are defined as facilities possessing any chemical of interest at quantities above the thresholds listed in Appendix A of the act. Because of this definition, CFATS also applies to entities outside the traditional chemical sector such as supply chain facilities and chemical end-users.

DHS uses a 4-level risk-based tiered structure for evaluating high-risk chemical facilities. As such, the security and protection of control systems in chemical manufacturing and storage facilities must be assessed and elevated commensurate with the proper DHS Threat Tier to prevent unauthorized access, theft, release, and sabotage.

RBPS (8) Cyber of the act requires facilities to "Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls..., critical business systems, and other sensitive computerized systems;" The DHS has issued an RBPS guidance document that provides metrics by RBPS number and tier level, but these metrics are not requisite to regulatory compliance.

As many refineries and chemical plants must adhere to ISO/IEC 27001 (Annex A) Controls because of their international ownership, the NIST SP800-53 also has a cross table mapping to the ISO/IEC 27001, in Appendix H, "International Information Security Standards."

DHS also provides a document comparing fifteen complementary standards for various sectors including ISO 27001 and the NIST SP800-53, Revision3, titled "Catalog of Control System Security: Recommendations for Standards Developer," (CoR, Revision 7, April 2011). The primary established standards compared in this document are:

- NIST SP800-82
- NRC Regulatory Guide 5.71
- NERC CIP -002-009 Revisions 2 and 3
- DoDI 8500.2
- NIST SP800-53
- CFATS Risk Based Performance Standard (RBPS) 8
- ISO/IEC 15408 Revision 3.1
- Consensus Audit Guidelines 2.3.

CFATS RBPS elements are not currently addressed in this catalog, although DHS CSSP has prepared a RBPS CoR mapping and plans to include it in a future revision of the CoR.

Chemical Facility Security News is a Chemical Industry-specific blog maintained by Patrick J. Coyle and provides a balanced year-end, nongovernmental industry view on the current state of CFATS, pending and delayed legislative issues and regulations including chemical delisting, streamlined CFATS information processing, security requirements, Chemical Inspectors, and perceived ISCD Problems. This blogsite also provides a good running history of issues since July 2007.

More information about the CFATS program can be found at the DHS-ICSD CFATS Knowledge Center, Version 2.0.Chemical Sector training and Resources information website provides chemical specific information on tools, publications, and specific training directed to the Chemical Sector. For more information on training and tools and how to request additional documentation, please send an email to ChemicalSector@dhs.gov.

Comments and suggestions for the DHS CoR can be sent to CSSP@dhs.gov, attention CoR Comments.

What is ICS-CERT?

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

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

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

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

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. This coordinated disclosure process ideally allows time for a vendor to develop and release patches and for users to test and deploy patches prior to public disclosure of the vulnerability. While this process is not always followed for a variety of reasons, ICS-CERT continues to strive for this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at ics-cert@dhs.gov or toll free at 1-877-776-7585.

Notable Coordinated Disclosure Researchers

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

- Steven Seeley, ICSA-11-362-01 – SCADATec SCADAPhone/Modubus TagServer Buffer Overflow, December 28, 2011
- Billy Rios and Terry McCorkle, ICSA-11-356-01 – GE Siemens Simatic HMI Authentication Vulnerabilities, December 22, 2011
- Celil Unuver (SignalSEC LLC), ICSA-11-355-01 – 7-Technologies IGSS Buffer Overflow, December 21, 2011
- Luigi Auriemma (ZDI), ICSA-11-355-02 – WellingTech Kingview, December 21, 2011
- UCQ (Cyber Defense Institute, Inc), ICSA-11-335-01 – 7-Technologies IGSS Data Server Buffer Overflow, December 20, 2011
- Carlos Mario Penagos Hollman of Synapse-labs, ICSA-11-314-01 – Safenet Sentinel and 7-T IGSS Input Sanitization vulnerability, December 12, 2011
- Kuang-Chun Hung (Morgan) (ICST), ICSA-11-340-01 – Arc Informatique PCVue Multiple Vulnerabilities, December 06, 2011
- Paul Davis, ICSA-11-298-01 – Sielco Systemi Winlog Buffer Overflow, December 06, 2011

Researchers Currently Working with ICS-CERT

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

Luigi Auriemma	Joel Langill	Rubén Santamarta	Dillon Beresford	Eireann Leverett
Secunia	Jeremy Brown	Yun Ting Lo (ICST)	Steven Seeley	Kuang-Chun Hung (ICST)
Terry McCorkle	UCQ	Paul Davis	Shawn Merdinger	Celil Unuver
Carlos Mario Penagos Hollmann	Michael Orlando	Knud Erik Højgaard (nSense)	Billy Rios	