ICS-CERT MONTHLY MONITOR

DECEMBER 2011

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

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

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

Illinois Water Utility Support

ICS-CERT deployed a fly-away team to Springfield, Illinois, in response to a possible cyber incident after an internal FOUO report titled "Public Water District Cyber Intrusion" was publicly disclosed.

This report was written and issued by the Illinois Statewide Terrorism & Intelligence Center (ISTIC) fusion center on November 10, 2011, detailing anomalous behavior in a supervisory control and data acquisition (SCADA) system at the Curran-Gardner water utility. The ISTIC report indicated that the water district had been the victim of a malicious cyber intrusion originating from a Russian IP address. More importantly, the ISTIC report seemed to indicate that the cyber attack was the root cause of a water pump failure.

The ICS-CERT contacted the water district on November 16 after learning of this report and offered support to help investigate the incident. Curran-Gardner requested onsite support to work with their team to analyze all available data. ICS-CERT deployed a fly-away team to the facility to perform onsite technical analysis in conjunction with the FBI and water district staff.

The ICS-CERT team performed an in-depth analysis, which included interviews with personnel and physical equipment inspections, in addition to network, affected hosts, and system logs analysis. The team's analysis turned up no evidence of a compromise, and all the foreign traffic was accounted for. The subsequent analysis by an independent inspector found evidence that the pump had failed as a result of physical and mechanical issues over a period of time rather than from a cyber attack.

The ICS-CERT has published an Information Bulletin titled "ICSB-11-327-01, Illinois Water Pump Failure Report" that can be downloaded from the ICS-CERT web page or directly at: http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf.

(continues on page 2)

NCCIC NEWS

ICS-CERT Supports NERC'S Gridex 2011

On November 16−17, 2011, ICS-CERT supported and participated in the North American Electric Reliability Corporation's (NERC's) cybersecurity incident readiness exercise, GridEx 2011. The GridEx 2011 exercise is part of NERC's ongoing cyber readiness program and was designed to test NERC's and the electricity industry's crisis response plans and validate current readiness in response to a cyber incident. In addition to ICS-CERT, more than 75 industry and government organizations participated in GridEx 2011 including NERC staff, the Electrical Sector Information Sharing and Analysis Center (ES-ISAC), regional entities, reliability coordinators, registered NERC entities, and federal agencies. ICS-CERT provided a variety of support functions for the exercise including planning, participation as a player, exercise inject development and release, and participation in the after-action analysis process. ICS-CERT anticipates continued collaboration with the electric power industry in future efforts to prepare for cybersecurity incidents.

ANNOUNCEMENTS

December Proclaimed Critical Infrastructure Protection Month

President Obama has proclaimed December 2011 as Critical Infrastructure Protection Month. DHS leads the critical infrastructure protection effort through a framework of public-private partnerships in close coordination with the 18 critical infrastructure sectors. More information regarding Critical Infrastructure Protection Month and related DHS programs can be found on the DHS website.

INCIDENT RESPONSE

Illinois Water Utility Support continued from page 1)

ICS-CERT is currently engaging with other groups within DHS, as well as state and local fusion centers, to evaluate lessons learned through this event and improve coordination and communications among stakeholders.

Organizations interested in creating or improving their incident response plans for control system environments may contact the ICS-CERT for resources and assistance. ICS-CERT also recommends reviewing the ICS-CERT Incident Handling Brochure at http://www.us-cert.gov/control_systems/pdf/Incident%20Handling%20Brochure-1.pdf.

Malware Analysis and Mitigation

ICS-CERT continues to assist the community with analyzing malware artifacts at an increasing rate. One of the factors in the increasing number of requests for assistance is that cybersecurity awareness has been on the rise. These requests have primarily been focused on ensuring that malware found residing on enterprise systems have not found their way onto control system networks, and if found, what is the most effective way of detection and removal. While few recent malwares making headlines have specifically targeted control systems, the trends indicated by these types of attacks represent are cause for concern. Regardless of the target, ICS security teams must deal with the reality of, and increase in frequency of attacks. They need to know how to manage and mitigate such incidents effectively. Teams responsible for ICS security must address the evolving sophistication of these threats within their operational limitations.

What can be done to decrease the impact of such attacks while increasing opportunities for timely detection? Below are some recommendations for minimizing the impact of malware and facilitating detection.

1. **Incorporate More Than Just Security Updates into the Patch Release Cycle—** Time to Live (TTL) applies to vulnerability exposure as well as to network packet transportation and real time operations. Reactive patching to address known vulnerabilities continues on as a staple mitigation technique in the security community. However, many teams still deploy only those patches and security updates that are deemed most critical by the vendor. Owners and operators of industrial control systems often face additional difficulties while trying to patch their systems, because of limitations imposed by the vendors of those systems concerning patches. However, when possible, asset owners and operators are encouraged to review optional or functional updates released by software vendors because these updates may increase security posture even though they don't resolve security vulnerabilities. Some of the updates that would help identify or mitigate the risk of certain malware include:
    a. Microsoft generally updates their root certificates as optional updates rather than critical updates, but failing to update the trusted certificates list on each host can have critical security impact.
    b. Other major applications that are critical dependencies for web browsing, etc., are also released under the optional updates. A prime example of this is the .Net Framework or Windows Media Player. Watch for these components because Microsoft bundles internally discovered vulnerabilities into service packs and product upgrades, rather than releasing the fixes through security patches, to minimize the patch management cycle. Skipping the optional updates can introduce vulnerabilities as significant as those addressed by security updates.
2. **Driver Signing—**Limit installation of driver files to those that are signed by a vendor

INCIDENT RESPONSE

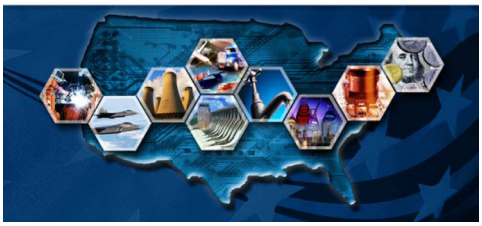
or are vetted by the ICS security team as being legitimate. Use directory services or local security policy to limit who (people, accounts, services) can install drivers and override the requirement for certified drivers. Make sure to log vetted driver files centrally and to have individual systems report when unsigned drivers are loaded into the operating system (OS). While there have been recent examples of malware using signed drivers to avoid detection, and though that trend is likely to continue, requiring drivers to be signed will greatly reduce a system's susceptibility to malware.

3. **Operating system partitioning**—Partitioning hard drives to separate the operating system, application functionality, or data storage can provide significant gains in security and performance. Should a critical system be infected with malware and require the operating system to be rebuilt, data stores on the second logical drive won't be impacted during the restoration. This segregation of functionality also makes it easier to create detection rules that are specific to data access and exfiltration rather than OS-specific tasks like system file integrity checking. While hard drive partitioning is not a substitute for a robust data backup policy, and also overlooks sophisticated persistence techniques, implementing a partitioned operating system is simple and pays great returns.
4. **File verification checks**—File verification checking, or use of a one-way hashing algorithm for verifying the integrity or authenticity of a computer file,[a] can add a great deal of security to critical systems as well as help troubleshoot functional incidents regarding corrupted files, etc. By incorporating file verification or integrity checking into the host-based monitoring process, administrators can identify when system files are changed and determine whether the changes were authorized and legitimate. File verification checking can generate a great deal of noise in log files so it is important to start monitoring systems that are relatively static, making industrial control systems a good place to monitor, as any changes will likely stand out.
5. **Registry differentials**—Malware often loads encrypted content into or otherwise modifies the infected system's registry. However, registry differentials can be performed to detect changes in the registry regardless of the malware's point of entry or impact. It may be worthwhile to perform periodic differentials on registry entries for critical systems and feed alerts into the host-based system monitoring data flow (if present) in order to detect potentially malicious changes to the system. As with file verification checking, performing registry differentials can take some time to set up and tune correctly. Start with performing the registry differentials on key systems or environments and integrate alert flagging into existing host-based monitoring systems to ease the transition for security administrators.
6. **Use of Attack Specific Detectors**—Antivirus and intrusion detection systems (IDS) regularly update their signature lists to detect known malware infections. However, some systems are incapable of running host-based malware detection and prevention software and may require stand-alone tools to detect the infection. Many stand-alone tools can be loaded directly onto systems, perform malware detection scans, and then be removed to prevent overloading the system or interfering with critical processes. Whitelisting solutions can help minimize malware attacks in these scenarios as well.

As always, the ICS-CERT stands by to provide support for critical infrastructure and ICS security teams. Please contact the ICS-CERT if you have questions or need further support.

a. File verification, http://en.wikipedia.org/wiki/File_verification, November 11, 2011.

UPCOMING EVENTS



JANUARY

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop
(1 week)
December 5–9, 2011
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

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

GLEG SCADA + PACK VERSION 1.8

ICS-CERT had published the ICS-CERT-11-230-01 alert titled "GLEG Agora SCADA + Exploit Pack Update 1.4" on August 18, 2011.

In that alert, ICS-CERT addressed GLEG's SCADA+ Exploit Pack, a package of add-ons for Immunity Inc.'s CANVAS framework. The SCADA+ Exploit Pack collection of exploits specifically targets industrial control systems (ICS) products. Publication of ICS products vulnerability exploits increases the ease with which an attacker could exploit these products.

Joel Langill, author of the SCADAHacker blog, provided a running synopsis of the several SCADA+ Exploit Packs in an Infosec Island article on December 5, 2011. That article covered versions up to and including the latest V1.8 updates.

The August alert included a table of affected vendors, products, vulnerability types, CVE (if known), and associated ICS-CERT products (if existing). ICS CERT has updated the vulnerability table to include seven of the nine vulnerabilities from SCADA+ Exploit Pack V 1.8, as identified in Langill's post.

Table 1. Exploit Pack vulnerability exploits.

Vendor	Product	Vulnerability Type	CVE	ICS-CERT Product
ARC Informatique	PcVue	Multiple	CVE-2011-4042 CVE-2011-4043 CVE-2011-4044 CVE-2011-4045	ICSA-11-340-01 ARC Informatique PcVue Multiple Vulnerabilities
Atvise WebMI	WebAccess	Multiple	Unknown	ICS-ALERT-11-283-02-Atvise webMI Multiple Vulnerabilities
Beckhoff	TwinCAT ENI Server 1.1.6.0	Denial of Service	CVE-2011-3486	ICSA-11-279-04-Beckhoff TwinCAT
GE	GE Intelligent Platforms Proficy Historian Data Archiver	Buffer Overflow	CVE-2011-1918	ICSA-11-243-03-GE Proficy Historian Data Archiver
GE	GE Intelligent Platforms Proficy Plant Applications	Buffer Overflow	CVE-2011-1919	ICSA-11-243-01-GE Proficy Plant Applications Buffer Overflow
MICROSYS, spol. sr.o	Promotic	Directory Traversal Stack Overflow Heap Overflow	Unknown	ICS-ALERT-11-286-01-Microsys, spol. sr.o Promotic
Open Automation Software	OPC Systems.Net Vulnerability	Malformed Packet	Unknown	ICS-ALERT-11-285-01-Open Automation Software OPC Systems NET Vulnerability

Organizations using any of the affected products should reference the ICS-CERT and/or CVE information available in Table 1 for information regarding patch availability and vulnerability impact. If no patch or solution that fully remediates the disclosed vulnerability is available from the product vendor, product users should work to implement relevant defensive measures including but not limited to defense-in-depth strategies.

b. http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-230-01.pdf, website last accessed December 13, 2011.

c. http://scadahacker.blogspot.com/2011/10/gleg-releases-ver-17-of-scada-exploit html, SCADhacker has a running update in his blog archive from V1.1 to V1.8; website last accessed December 13, 2011.

d. https://www.infosecisland.com/blogview/18505-Gleg-Releases-Version-18-of-the-SCADA-Exploit-Pack html, website last accessed December 13, 2011.

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-11-333-01—Microsys Promotic Vulnerability"

ICS-CERT is aware of a public report of a use-after-free vulnerability with proof-of-concept (PoC) exploit code affecting MICROSYS, spol. s r.o. PROMOTIC, a SCADA HMI product. According to this report, the vulnerability is exploitable when the program terminates due to an error during the loading of a specially crafted project file. 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 not yet verified the vulnerabilities or PoC code, but 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-11-332-02—Siemens SIMATIC WinCC Flexible"

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting Siemens SIMATIC WinCC Flexible Runtime, a human-machine interface product. According to this report, the vulnerabilities are exploitable remotely 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-11-332-03—Optima APIFTP Server"

ICS-CERT is aware of a public report of denial-of-service vulnerabilities with proof-of-concept (PoC) exploit code affecting Optima APIFTP Server, part of a suite of supervisory control and data acquisition/ human-machine interface products. According to this report, these vulnerabilities are exploitable by sending specially crafted packets to the server on Port 10260/UDP. This report was released Luigi Auriemma without coordination with ICS-CERT, the vendor, or other coordinating entity of which ICS-CERT is aware.

ICS-CERT has coordinated the report with Optima, which 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-11-332-01—Siemens Automation License Manager"

ICS-CERT is aware of a public report of four vulnerabilities with proof-of-concept (PoC) exploit code affecting Siemens Automation License Manager, a supervisory control and data acquisition/ human-machine interface product. 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 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-11-306-01—Advantech WebAccess ActiveX Vulnerability"

ICS-CERT is aware of a public report detailing an ActiveX vulnerability with proof-of-concept (PoC) exploit code, affecting Advantech Broadwin WebAccess, a supervisory control and data acquisition/ human-machine interface (SCADA/ HMI) product. According to this report, this vulnerability is exploitable by a combination of ActiveX methods. This report was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has not yet verified the vulnerabilities or PoC code, but 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-11-291-01E—(UPDATE) W32 Duqu-malware"

This updated Alert is the final of a series of six ICS-CERT Alerts about W32.Duqu. On November 1, 2011 Symantec and the Laboratory of Cryptography and Systems Security (CrySyS) released updated reports identifying possible affected organizations, the dropper used to infect systems and a new command and control (C&C) IP address. ICS-CERT is in the process of compiling and re-organizing available data for release in an upcoming advisory. According to Symantec, they have confirmed six possible infected organizations in eight countries including France, Netherlands, Switzerland, Ukraine, India, Iran (2), Sudan, and Vietnam. Symantec notes the organizations are only traceable back to an ISP. Other security vendors have reported infections in Austria, Hungary, Indonesia, United Kingdom, and Iran. At this point, a comprehensive list of infected organizations is not available. As of October 21, 2011, there have been few infections and no evidence based on current code analysis that Duqu presents a specific threat to ICSs.

ADVISORIES

Advisory "ICSA-11-307-01—Schneider Electric Vijeo Historian Web Server Multiple Vulnerabilities"

ICS CERT originally released Advisory ICSA-11-307-01P on the US-CERT secure Portal on November 03, 2011. This web page release was delayed to allow users sufficient time to download and install the update. Researcher Kuang-Chun Hung of Security Research and Service Institute, Information and Communication Security

RECENT PRODUCT RELEASES

Technology Center (ICST) has identified four vulnerabilities in the Schneider Electric Vijeo Historian product line. These vulnerabilities include a denial of service (DoS), buffer overflow, a cross-site scripting (XSS), and a directory traversal.

ICS-CERT has coordinated this report with Schneider Electric and ICST. Schneider has produced a fix that resolves these vulnerabilities. ICST has tested this fix and validated that it fully resolves these vulnerabilities

Advisory "ICSA-11-319-01—InduSoft Web StudioMultiple Vulnerabilities"

ICS-CERT has become aware of a report from the Zero Day Initiative (ZDI) concerning two vulnerabilities in the InduSoft Web Studio software. This information was reported to ZDI by independent security researcher Luigi Auriemma.

These vulnerabilities exploit unauthenticated remote code execution within the CEServer Operation and the CEServer.exe directories.

ZDI has coordinated with InduSoft, who has produced a patch that mitigates these vulnerabilities. ICS CERT has not validated the patch.

Advisory "ICSA-11-279-02—CitectSCADA and Mitsubishi MX4 SCADA Batch Server Buffer Overflow"

ICS CERT originally released Advisory ICSA-11-279-02P on the US-CERT secure Portal on October 06, 2011. This web page release was delayed to allow users time to download and install the update. Researcher Kuang-Chun Hung of Taiwans Information and Communication Security Technology Center (ICST) has reported a buffer overflow affecting Mitsubishi MX4 Supervisory Control and Data Acquisition (SCADA). Upon further investigation, MX4 SCADA was found to be a version of CitectSCADA, a product offered by Schneider Electric. This Advisory includes a full list of known affected products.

This buffer overflow vulnerability resides in a third-party component used by the CitectSCADA and MX4 SCADA Batch products. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code.

ICS-CERT has coordinated the researchers vulnerability report with Schneider Electric. Schneider Electric has issued a patch to address the reported vulnerability. The researcher has confirmed the patch is effective in addressing the vulnerability. Schneider Electric has provided the patch to Mitsubishi for distribution to MX4 SCADA customers.

Advisory "ICSA-11-094-02A—Broadwin WebAccess RPC Vulnerability"

This Advisory Update is a follow-up to the original Advisory titled ICSA-11-094-02 "Advantech/BroadWin WebAccess RPC Vulnerability" that was published April 4, 2011, on the ICS-CERT web page. That Advisory was preceded by Alert ICS-ALERT-11-081-01 "BroadWin WebAccess" where independent security researcher Ruban Santamarta had identified details and released exploit code for a Remote Procedure Call (RPC) vulnerability in Advantech/BroadWin WebAccess. There were three updates to this advisory as follows:

1. Advantech/BroadWin has notified ICS-CERT that a patch will not be issued to address this vulnerability.
2. CVE-2011-4041chas been assigned to this vulnerability in the National Vulnerability Database.
3. Advantech Broadwin has no plans to issue a patch to address this vulnerability.

Advisory "ICSA-11-243-03—GE Intelligent Platforms Proficy Historian Data Archiver Buffer Overflow Vulnerability"

ICS CERT originally released Advisory ICSA-11-243-02P on the US-CERT secure Portal on August 31, 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 multiple cross-site scripting (XSS) vulnerabilities in the GE Intelligent Platforms Proficy Historian Web Administrator software.

ICS-CERT has coordinated this vulnerability with GE and the researchers, and GE has made recommendations to reduce the potential attack surface. The affected product, Historian Web Administrator with Proficy Historian, is considered by GE to be a legacy component; as a result, GE is not issuing a patch for this vulnerability.

Advisory "ICSA-11-243-01—GE Proficy Plant Applications Buffer Overflow"

ICS CERT originally released Advisory ICSA-11-243-02P on the US-CERT secure Portal on August 31, 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 GE concerning a stack-based buffer overflow vulnerability in the GE Intelligent Platform Proficy Plant Applications software suite.

ICS-CERT has coordinated with GE Intelligent Platforms to validate this vulnerability, and GE has created a patch to address the issue. ICS-CERT has validated that the patch fully resolves this issue.

Advisory "ICSA-11-243-02—GE Proficy Historian Web Administrator XSS"

ICS CERT originally released Advisory ICSA-11-243-02P on the US-CERT secure Portal on August 31, 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 multiple cross-site scripting (XSS) vulnerabilities in the GE Intelligent Platforms Proficy Historian Web Administrator software.

ICS-CERT has coordinated this vulnerability with GE and the researchers, and GE has made recommendations to reduce the potential attack surface. The affected product, Historian Web Administrator with Proficy Historian, is considered by GE to be a legacy component; as a result, GE is not issuing a patch for this vulnerability.

RECENT PRODUCT RELEASES

OTHER

"ICSB 11-327-01 - Information Bulletin"

On November 10, 2011, the Illinois Statewide Terrorism & Intelligence Center (STIC) issued a Daily Intelligence Notes report entitled "Public Water District Cyber Intrusion." As widely reported in the press, the report detailed initial findings of anomalous behavior in a supervisory control and data acquisition (SCADA) system at a Central Illinois public water district. This report also alleged a malicious cyber intrusion from an IP address located in Russia that caused the SCADA system to power on and off, resulting in a water pump burnout.

ICS-CERT was made aware of the report on November 16, 2011, and immediately reached out to the STIC to gather additional information. ICS-CERT was provided with a log file; however, initial analysis could not validate any evidence to support the assertion that a cyber intrusion had occurred. 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 Curran-Gardner Public Water District in Springfield, Illinois. 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 inspections, and collect logs and artifacts for analysis.

No evidence supports claims made in the initial Illinois STIC report "which were based on raw, unconfirmed data and subsequently leaked to the media" that any credentials were stolen, or that the vendor was involved in any malicious activity that led to a pump failure at the water plant. DHS and the FBI have concluded that there was no malicious or unauthorized traffic from Russia or any foreign entities, as previously reported.

Analysis of what caused the pump to fail is ongoing. ICS-CERT will continue to coordinate with the FBI, Water ISAC, MS-ISAC and other organizations as appropriate.

Advisory "JSAR-11-312-01 - W32.Duqu-malware"

This Joint Security Awareness Report (JSAR) provides follow-up information and independent analysis from ICS-CERT and US-CERT about the W32.Duqu Malware.

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 Obama administration wants hackers to be prosecuted under the same laws used to target organized crime

2011-11-28

The Obama administration is seeking tougher sentences for people who are found guilty of hacking or other digital offenses, two officials said Wednesday.

Associate Deputy Attorney General James Baker and Secret Service Deputy Special Agent in Charge Pablo Martinez said the maximum sentences for cyber crimes have failed to keep pace with the severity of the threats.

Martinez said hackers are often members of sophisticated criminal networks.

http://newworldorderreport.com/News/tabid/266/ID/8604/The-Obama-administration-wants-hackers-to-be-prosecuted-under-the-same-laws-used-to-target-organized-crime.aspx

Hackers target IPv6

2011-11-28

If your IPv6 strategy is to delay implementation as long as you can, you still must address IPv6 security concerns right now. If you plan to deploy IPv6 in a dual-stack configuration with IPv4, you're still not off the hook when it comes to security. And if you think you can simply turn off IPv6, that's not going to fly either.

http://www.computerworld.com/s/article/9222183/Hackers_target_IPv6

Software Assurance Metrics and Tool Evaluation (SAMATE) Reference Dataset

2011-11-28

Want to avoid software snafus? Here's a good place to start. The Software Assurance Metrics and Tool Evaluation (SAMATE) Reference Dataset contains examples of errors in a number of popular programming languages that could leave software vulnerable to exploits by hackers and criminals.

http://gcn.com/articles/2011/11/28/nist-samate-avoid-software-snafus.aspx

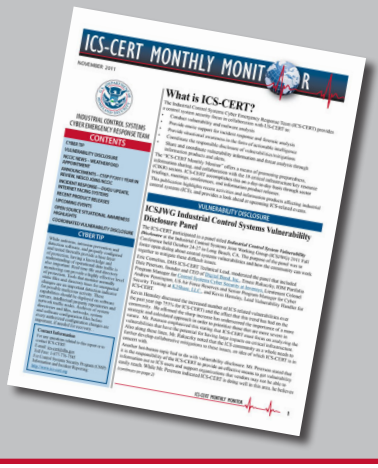
http://samate nist.gov/SRD/

Four Hack Suspects Linked to Terrorist Group

2011-11-27

The FBI and Philippine law enforcement officials arrested four people in the Philippines this week who were allegedly paid by terrorists to hack into AT&T's system, but the company said its system was not breached.

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



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. 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

The four, who were arrested Wednesday in Manila, were paid by the same Saudi Arabian-based terrorist group identified by the FBI as funding the 2008 attack on Mumbai, the Philippines' Criminal Investigation and Detection Group (CIDG) said in a statement. The coordinated attacks in India's largest city claimed 164 lives and wounded at least 308.

"The hacking activity resulted in almost $2 million in losses incurred by the company," the CIDG said in a statement.

http://news.cnet.com/8301-1009_3-57331688-83/four-hack-suspects-linked-to-terrorist-group/

Gleg releases Ver 1.8 of the SCADA+ Exploit Pack for Immunity Canvas

2011-11-27

On November 24, Gleg released version 1.8 of the SCADA+ Exploit Pack for the Immunity Canvas framework, along with a corresponding version 2.7 of the Agora Exploit Pack.

http://scadahacker.blogspot.com/2011/11/gleg-releases-ver-18-of-scada-exploit html

Ageing control systems expose utilities to hack attacks

2011-11-23

Claims that hackers attacked two US water companies have focused attention on the computer systems behind the fabric of everyday life.

http://www.bbc.co.uk/news/technology-15845672

Was The Three Character Password Used To Hack South Houston's Water Treatment Plant A Siemens Default?

2011-11-22

Siemens said on Tuesday that it is working with the U.S. Department of Homeland Security to investigate a cyber intrusion into a water treatment plant in South Houston, Texas, but couldn't confirm that a default, three digit password hard coded into an application used to control the company's SCADA software played a role.

http://threatpost.com/en_us/blogs/was-three-character-password-used-hack-south-houstons-water-treatment-plant-siemens-default-11

No evidence of cyberattack at water pump, DHS says

2011-11-22

Federal investigators have found no evidence that a cyberattack was behind a water pump failure this month in Illinois, the government announced Tuesday.

http://www.cnn.com/2011/11/22/us/cyberattack-investigation/index.html

Cybersecurity expert hails new DHS cyber chief

2011-11-22

New Department of Homeland Security Deputy Undersecretary for Cybersecurity Mark Weatherford's arrival could "herald an era of greater balance in national cybersecurity leadership" between DHS and the intelligence community, according to a prominent cybersecurity expert.

http://thehill.com/blogs/hillicon-valley/technology/195145-cybersecurity-expert-hails-new-dhs-cyber-chief

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Lax security at Nasdaq helped hackers

2011-11-17

A federal investigation into last year's cyber attack on Nasdaq OMX Group found surprisingly lax security practices that made the exchange operator an easy target for hackers, people with knowledge of the probe said. The sources did not want to be identified because the matter is classified.

http://uk reuters.com/article/2011/11/17/us-nasdaq-cyber-idUKTRE7AG2NU20111117

Mobile devices, virtualization seen as biggest security challenges: Ponemon survey

2011-11-16

Increased use of mobile devices, especially smartphones, in addition to the transition to virtualization, are key factors weighing on enterprises trying to sort out security strategy and budgets, according to a survey of 688 information and security managers.

http://www.computerworld.com/s/article/9221924/Mobile_devices_virtualization_seen_as_biggest_security_challenges_Ponemon_survey

Employees' Droids among biggest government cyber menaces

2011-11-15

In 2012, agencies should worry about hackers attacking the growing number of federal employees toting their own iPhones and Droids to work, according to a forecast of next year's greatest cyber dangers compiled by M86 Security Labs.

http://www nextgov.com/nextgov/ng_20111115_9168.php

Hackers may have spent years crafting Duqu

2011-11-11

Gang customized attack files for each target, says Kaspersky Lab.

The hacker group behind Duqu may have been working on its attack code for more than four years, new analysis of the Trojan revealed Friday.

http://www.computerworld.com/s/article/9221760/Hackers_may_have_spent_years_crafting_Duqu

Vendors under pressure to better secure IT supply chain

2011-11-09

Lawmakers want vendors to take more responsibility to secure the government's technology supply chain.

http://www federalnewsradio.com/?nid=241&sid=2625581

Microsoft issues workaround for Duqu attack while it prepares a patch

2011-11-04

Microsoft has published code to temporarily blunt attacks against a software vulnerability exploited by Duqu, an advanced piece of malicious software still being closely analyzed by security researchers.

Microsoft is working on a patch for the vulnerability in the Win32k TrueType font parsing engine, a component of various Windows operating systems. An attacker could exploit it to load malicious code on a computer in kernel mode.

http://www.computerworld.com/s/article/9221491/Microsoft_issues_workaround_for_Duqu_attack_while_it_prepares_a_patch

http://technet microsoft.com/en-us/security/advisory/2639658

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Kaspersky and cyber terrorism

2011-11-04

Of all the pronouncements coming out of the London Cyber Summit this week, the statements of Eugene Kaspersky are the most provocative. Rather than pile on and criticize him for uttering the words "cyber terrorism" it is worth taking a deep breath and considering what could give rise to his statements.

http://www.dos-protection.co.uk/?p=59

NIST releases new Smart Grid roadmap

2011-11-04

The National Institute of Standards and Technology is helping to change the way your office obtains and uses electricity. NIST has released a new roadmap for building the Smart Grid, adding a new list of standards, cybersecurity guidance and product testing proposals.

http://www federalnewsradio.com/?nid=241&sid=2620188

Report: Russia and China are top thieves of U.S. technology

2011-11-03

For the first time, the United States is publicly accusing China and Russia of being the top offenders in the theft of U.S. economic and technology information, according to an intelligence report released Thursday.

http://www.cnn.com/2011/11/03/us/china-russia-industrial-espionage/index.html?hpt=us_c2

'Nitro' hackers use stock malware to steal chemical, defense secrets

2011-10-31

Attackers used an off-the-shelf Trojan horse to sniff out secrets from nearly 50 companies, many of them in the chemical and defense industries, Symantec researchers said today.

http://www.computerworld.com/s/article/9221335/_Nitro_hackers_use_stock_malware_to_steal_chemical_defense_secrets

http://gcn.com/articles/2011/11/01/cyber-spy-attacks-target-chemical-industry.aspx

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:

- Kuang-Chun Hung (Morgan) (ICST), ICSA-11-307-01 – Schneider Electric Vijeo Historian Web Server, Nov 28
- Kuang-Chun Hung (Morgan) (ICST), ICSA-11-279-02 – CitectSCADA and Mitsubishi MX4 SCADA Batch, Nov 08
- Rubén Santamarta, ICSA-11-094-02A – Advantech/BroadWin WebAccess, Nov 04
- Billy Rios and Terry McCorkle, ICSA-11-243-02 – GE Intelligent Platforms Proficy Historian Web Administrator, Nov 01
- Billy Rios and Terry McCorkle, ICSA-11-243-01 - GE Intelligent Platforms Proficy Plant Applications Buffer, Nov 01

Researchers Currently Working with ICS-CERT

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

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