ICS-CERT MONITOR

January/February/March 2013

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

INCIDENT RESPONSE ACTIVITY

SITUATIONAL AWARENESS

ICS-CERT NEWS

RECENT PRODUCT RELEASES

NOTEWORTHY NEWS HIGHLIGHTS

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

INCIDENT RESPONSE ACTIVITY

ATTACKER LEVERAGES PUBLIC INFORMATION TO CUSTOMIZE SPEAR-PHISHING CAMPAIGN

A recent spear-phishing campaign started and ended in October 2012, using publicly available information from an electric utility's Web site to customize an attack against members of the Energy Sector. Employee names, company email addresses, company affiliations, and work titles were found on the utility's Web site on a page that listed the attendees at a recent committee meeting. This publicly available information gave the attacker the company knowledge necessary to target specific individuals within the electric sector.

Malicious emails were crafted informing the recipients of the sender's new email address and asked them to click on the attached link. This link led to a site that contained malware. Another email with a malicious attachment may also have been associated with this campaign.

Working with the ES-ISAC, it was determined that 11 entities were targeted in this campaign, and luckily no known infections or intrusions occurred. ICS-CERT worked with our partners at the ES-ISAC to coordinate support for the targeted entities. Additional information about this event can be found on the US-CERT Control systems secure portal (ICS-ALERT 12 279 01P, October 05, 2012).

Publicly accessible information commonly found on social media, as well as professional organization and industry conference Web sites, is a recognized resource for attackers performing reconnaissance activities. With this information, attackers can craft convincing spear phishing and have a higher likelihood of successfully convincing the targeted individual to click on the malicious link or attachment.

In order to reduce the likelihood of becoming a victim of spear-phishing attacks, minimize the business-related and personal information on social media Web sites. Business-related information could include job title, company email, organizational structure, and project names. If information exists on other Web sites, contact the Web site owner and ask that it be removed.

ICS-CERT recommends that users not click on Web links or open attachments from unsolicited emails. Users should delete these emails and report them to their helpdesk or computer security group. For more information on avoiding social engineering and phishing attacks, refer to Security Tip ST04-014. Please contact ICS-CERT at ics-cert@hq.dhs.gov for further information on spear phishing or more tips on how to protect against spear phishing.

Contact Information

For any questions related to this report or to contact ICS-CERT:
Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: http://www.ics-cert.org.

INCIDENT RESPONSE ACTIVITY - Continued

COMPROMISE VIA "CREDENTIAL STORAGE" VULNERABILITY

ICS-CERT recently learned of an incident that occurred early last year involving hackers who penetrated the building energy management system (EMS) of a New Jersey manufacturing company. According to the source, intruders successfully exploited a weak credential storage vulnerability to access the organization's Tridium Niagara AX building EMS. The intruders were able to identify the Internet facing devices using the SHODAN search engine and compromised the system by taking advantage of weak authentication credentials.

The incident in New Jersey was similar to another incident that occurred in early 2012 where a state government facility's building EMS was also compromised. In this incident, the facility was compromised by an intruder who was able to exploit weak authentication settings on the system's Internet-accessible Niagara interface and manipulate set points to change the temperature settings. (see February 2012 Monthly Monitor).

On August 15, 2012, Tridium issued a security patch along with additional mitigation steps for users of Niagara AX Framework. But the incidents cited above underscore the need for Internet-facing devices to be properly secured against intruders, particularly in light of the SHODAN search engine.

Security researchers Billy Rios and Terry McCorkle had notified ICS-CERT of weak credential storage vulnerabilities and exploit code for Tridium Niagara in 2012. ICS-CERT contacted Tridium, which developed and issued the patch along with a security advisory detailing mitigation steps for their customers. ICS-CERT released ICSA-12-228-01 – Tridium Niagara Multiple Vulnerabilities, on August 15, 2012.

In addition to applying the available security patch from Tridium, which prevents access to the config.bog file and backups of the file from network facing clients, ICS-CERT and Tridium recommended the following mitigations:

- To mitigate the decoding of passwords listed in the config.bog file, Tridium recommends that security settings for file access be assigned only at the administrator level.
- Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts.
- Use strong passwords.
- Change default credentials.
- Limit user access to the file system following the instructions in the Niagara AX Framework.
- Ensure that control systems are not directly Internet facing.

Tridium Niagara AX software is used in applications that include energy management, building automation, telecommunications, security automation, and total facilities management applications.

WATERING HOLE ATTACKS

In early January 2013, ICS-CERT became aware of and issued an alert to warn of watering hole attacks that used two vulnerabilities, including a zero-day (0-day) vulnerability affecting Microsoft Internet Explorer (IE), Versions 6, 7, and 8.

This zero-day was reportedly being used in at least two watering hole attacks against the Council of Foreign Relations (CFR) and Capstone Turbine Corporation where attackers compromised the Web sites with malware in order to target visitors of those Web sites.

Watering hole attacks involve compromising legitimate Web sites with malware in an attempt to infect visitors of those sites. Web sites thought to be of interest to particular organizations are often chosen in the hopes that end-users will visit them and become infected with malware. According to various reports,[1] watering hole attacks have been used in previous attacks by sophisticated threat actors to gain access to a victim's computer. ICS-CERT was concerned that this attack technique could be leveraged by sophisticated attacks to target critical infrastructure asset owners.

Upon learning of the attacks, ICS-CERT reached out to CFR and Capstone Turbine Corporation to notify them of the malware and find out if any asset owners visited the Web pages while they were infected. ICS-CERT continues to evaluate this incident and has learned of numerous asset owners across multiple sectors who were compromised as a result of these attacks. Both CFR and Capstone Turbine Corporation removed the malware, and Microsoft has since issued a security bulletin and an out of band security update to resolve the vulnerability.

ICS-CERT published an alert to the portal to warn of the activity and provide indicators of compromise. Asset owners and operators of critical infrastructure can request access to the Secure Portal to request access to this and other important alerts and advisories.

ICS-CERT recommends that organizations review their policies and requirements for browsing software and ensure common office system applications are up to date. Information Technology staff are advised to monitor application vendors for "out-of-band" patch notifications and updates. If your company has been exposed to malware of any kind and would like ICS-CERT assistance, please call 877-776-7585.

1. Symantec Blog, http://www.symantec.com/connect/blogs/internet-explorer-zero-day-used-watering-hole-attack-qa, Web site last accessed January 3, 2013

SITUATIONAL AWARENESS

CSET® 5.0 RELEASED – UPDATED SUPPORT TO PROTECT CRITICAL ASSETS

In dynamically changing technological societies, rapidly evolving cyber threats continue to challenge the nation's critical infrastructure defense strategies. Addressing these ongoing threats demands better tools and processes to assist asset owners in confronting and surviving the world of cyber attacks. DHS has developed the Cyber Security Evaluation Tool® (CSET®) Version 5.0, which is designed to assist organizations in assessing their security practices and identifying potential cybersecurity risks and gaps that exist within their current control system networks. The assessment results assist users in establishing a baseline cybersecurity posture and identify areas for improvement.

CSET® Version 5.0 provides a systematic and comprehensive approach for improving cybersecurity strategies and techniques. It allows users to "benchmark" critical control systems against nationally recognized cybersecurity standards and guidelines, including existing sector standards. This provides users the assurance that the same approach to cyber resilience is being used and communicated across the industrial control systems community. It assists asset owners in identifying potential vulnerabilities while establishing an effective path forward for improving overall cybersecurity and defense-in-depth techniques.

Numerous organizations within the US Critical Infrastructure Sectors have already used the CSET® process to identify weaknesses and vulnerabilities within their control system networks–from weak authentication techniques to ineffective patch management processes. The CSET® assisted these organizations in identifying and prioritizing their most critical vulnerabilities requiring immediate attention and provided real time resolutions and recommendations for enhancing their security awareness and defensive posture.

By leveraging the expertise and experience of different individuals within ICS-CERT, the working knowledge of vulnerabilities and cybersecurity incidents can be passed directly to asset owners and operators. The vulnerability and incident handlers share their experiences and pass along knowledge that can be used to secure the site in the event of an incident.

ICS-CERT also maintains incident response expertise and deploys teams on site to assist asset owners during a cyber attack or intrusion event.

During the past 12 months, DHS has worked effectively with asset owners in all sixteen US Critical Infrastructure Sectors in nearly every state, completing over 80 individual assessments, improving their cybersecurity posture and awareness through the implementation of the CSET® and other DHS onsite cyber assessment assistance. By using the CSET® assessment process, users have been able to gain momentum toward implementing cybersecurity processes within their facilities in an effort to achieve a more secure control system environment.

Asset owners and operators who have not taken advantage of the CSET® assessment capabilities are encouraged to do so. The CSET® tool can be downloaded free of charge from the ICS-CERT Web site: http://www.us-cert.gov/control_systems/satool html.
If onsite assistance in using CSET® is needed, delivery of a CD copy of the tool or further information can be requested by contacting cset@hq.dhs.gov.

MULTIYEAR ASSESSMENTS REVEAL COMMON VULNERABILITIES

ICS-CERT recently completed 3 years of onsite assessments for over 230 critical asset owners to identify security gaps in their enterprise and control system networks. ICS-CERT provides support to assist and enhance review of existing customer systems to discover possible vulnerabilities as well as developing strategies for effective defense-in-depth processes. These assessments provided awareness of national cybersecurity standards, industry-based recommendations and best practices and were intended to strengthen the nation's ICS security posture for critical infrastructure control system owners, operators, and control system manufacturers.

These assessments were performed using the Cyber Security Evaluation Tool® (CSET®) and compared each organization's security practices against industry cyber standards. Based on these studies, ICS-CERT compiled a list of the most common cybersecurity gaps and vulnerabilities identified.

As part of the strategy to assist industry with securing critical control systems, onsite consultations using the CSET® as guidance are offered at no cost to asset owners and provide an opportunity to examine an organization's cybersecurity posture with the assistance of the Department of Homeland Security's (DHS's) cybersecurity subject matter experts.

SITUATIONAL AWARENESS - Continued

Based on the findings uncovered during the CSET® evaluations, vulnerabilities and security gaps were identified within asset owner facilities and documented as common cybersecurity gaps. The assessments also assisted these organizations in identifying and prioritizing their most critical vulnerabilities requiring immediate attention and provided real time resolutions and recommendations for enhancing their security awareness and defensive posture.

Table 1 ranks the top three security gap areas identified during the assessments.

Table 1. Most common weaknesses identified from CSET® assessments

CSET® Gap Areas
Lack of formal documentation
Audit and Accountability (Event Monitoring)
Permissions, Privileges, and Access Control

Table 2 identifies the common security weakness identified during CSET® assessments and presents common security weaknesses identified during onsite CSET® assessments.

Category	Common Vulnerability
Permissions, Privileges, and Access Controls	• Poor system access controls
Improper Authentication	• Poor system identification/authentication controls
Credentials Management	• Insufficiently protected credentials • Weak passwords
Security Configuration and Maintenance	• Weak testing environments • Poor patch management, limited patch management abilities • Weak backup and restore capabilities
Planning/Policy/Procedures	• Poor security documentation and maintenance • Lack of formal documentation • Insufficient disaster recovery penetration
Network Design Weaknesses	• Common ICS network design weaknesses • No security perimeter defined • Lack of network segmentation • Lack of functional DMZs • Firewalls nonexistent or improperly configured
Network Component Configuration (Implementation Vulnerabilities)	• Network devices not properly configured • Port security not implemented on network equipment • Lack of or poor monitoring of intrusion detection systems (IDSs)
Audit and Accountability (Event Monitoring)	• Lack of security audits/assessments • Lack of logging or poor logging practices • Network architecture not well understood • Weak enforcement of remote login policies • Weak control of incoming and outgoing media

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

SITUATIONAL AWARENESS - Continued

ICS-CERT encourages asset owners to review their network for these common security gaps and take measures to eliminate known system vulnerabilities. Security is a continuous process and should be included as a key element in every organization's operational plans and policies.

Asset owners and operators who would like to inquire about CSET® assessment capabilities are encouraged to visit http://ics-cert.us-cert.gov/satool.html or contact cset@hq.dhs.gov. The CSET® tool can also be downloaded free of charge from the link listed above.

PROTECTING CREDENTIALS FROM COMPROMISE

Protection of user logon credentials is an important consideration for security professionals tasked with defending their networks from sophisticated intrusions. Protecting credentials can help limit the extent of an intrusion and prevent lateral movement from occurring. Common tactics employed by attackers to compromise credentials include brute force cracking of password hashes and a technique referred to as "pass-the-hash."

Brute force cracking requires the attacker to "guess" the original password by systematically hashing and comparing the results of possible passwords. When a match is found, then a usable password has been identified. This process is greatly expedited through the use of "rainbow tables," or large tables of precomputed hashes. The pass-the-hash technique involves using cached password hashes extracted from the memory of a victim machine to gain access to additional machines in the domain.

The following two subsections describe mitigation techniques to reduce the possible vectors that attackers can use to compromise these credentials and reduce the locations that the stolen credential can be used to spread through the network. In addition to these two techniques, Microsoft has also released guidance that discusses methods for protecting user credentials that administrators should consult. You should evaluate each of these techniques and possible side effects before making any changes to your systems.

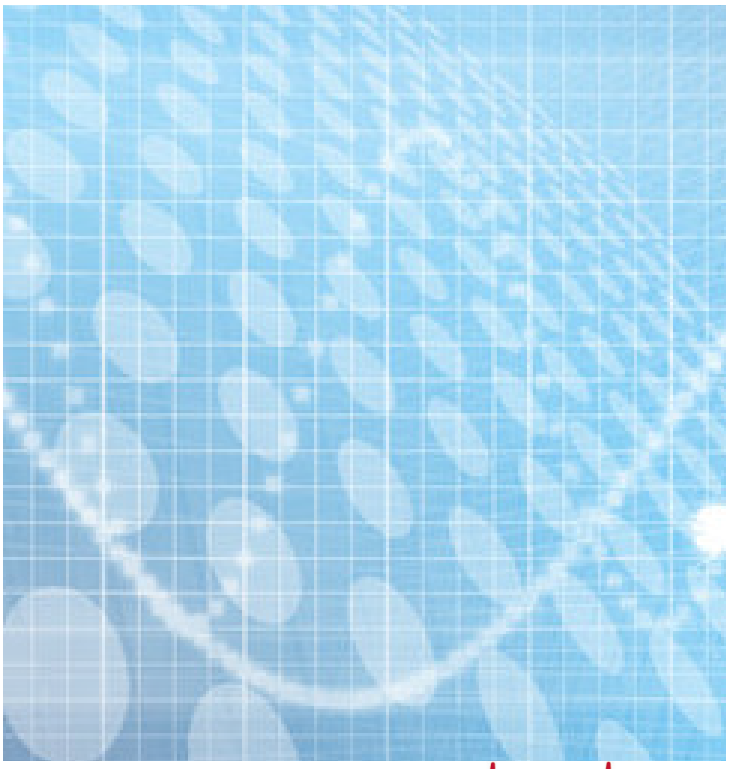
Proper Permission Management

Establish an appropriate privileged account hierarchy for administrative accounts (e.g., Enterprise Administrator, Domain Administrator, help desk accounts). The proper hierarchical design involves administrative rights and administrative responsibility being inversely proportional to each other. For example, Domain Administrators (one of the most privileged accounts) should only be used to administer the domain controllers, while a help desk account (an account with several task responsibilities) should have few administrative rights. This approach should include decisions about which hosts the accounts can be used and the manner in which the administrator accesses the devices. Exceptions to these policies are best supported with the creation of temporary accounts that are removed after the task is completed or through the use of designated management machines that are heavily restricted using ACLs (access control lists) and IPSec. These approaches make the Domain Administrator account, Enterprise Administrator account, domain controller, exchange server, and other high value targets more difficult for attackers to compromise.

> Note: Newer versions of Windows provide for greater levels of granularity by which privileges can be assigned, thereby enabling better silos to safeguard permissions.

Carefully consider the decision to grant users administrative rights to their machines. Execution of basis processes, such as Web browsing or reading email as an administrator, puts the machine at greater risk of compromise and losing control of its cached credentials.

Restrict the use of SeDebugPrivilege to those users who actually need it. This privilege can be used to perform DLL injection, a technique used by the majority of the pass-the-hash tools and other malware. By default, this is often assigned to the Administrators group, but consider being more restrictive. Create a specific debug user, and assign this account the right to use the privilege via the "run as" command, thereby gaining temporary privilege escalation.



SITUATIONAL AWARENESS - Continued

Network/System Design and Policies

Apply the principle of Internet, DMZ, and intranet zones throughout the network to isolate different trust sectors. Few reasons exist for one workstation to talk to another workstation or for it to talk to all the servers. Arrange infrastructure devices and software to create security zones to group users needing to communicate with each other. This technique helps to slow or prevent lateral movement throughout the rest of the network. Host-based firewalls that restrict incoming connections are another method for impeding unneeded interhost communication.

Exercise caution when using a common baseline image where company workstations and active local user accounts are present on the same machine. In this situation, all images will share the same password, this is especially damaging if the local administrator accounts have not been disabled. Using these common credentials, an attacker could quickly compromise all the machines loaded with this image. For this reason, IT administrators should consider disabling, changing, or removing local machine accounts to ensure that local accounts across the network have unique passwords.

Require the rebooting of all machines immediately after use by a privileged user. This clears the user's credentials from memory, a common target for pass-the-hash tools.

ICS-CERT also recommends that organizations move away from using LAN Manager (LM) hashes where possible. LM hashes are inherently weak and can be broken relatively quickly, allowing an adversary to use the actual password instead of relying on a pass-the-hash attack. Not all companies will be able to make this switch as some legacy systems are incompatible, but every effort should be used to migrate away from these systems in order to increase the networkwide security posture.

Note: When performing a global password reset, network managers should at the same time disable LM hashes to avoid the need for another global password reset when that method of password storage is disabled.

Organizations should consider moving to a multifactor authentication system (e.g., SmartCards) or ensure that users choose complex passwords and change them regularly.

ICS-CERT NEWS

ICS-CERT CONSOLIDATES MISSION SUPPORT

A recent DHS realignment has consolidated the mission support services that were formerly associated with the Control Systems Security Program (CSSP) and rolled them up to fall under the umbrella as ICS-CERT. This allows ICS-CERT to provide a full spectrum of control systems security products and services as it executes its mission and partnership with the ICS stakeholder community. All the services offered under the CSSP such as training, the Cyber Security Evaluation Tool (CSET®), onsite assessments, the ICSJWG forum, and more will still be available in addition to ICS-CERT's operational services such as incident response and analytic support services. For more information about all the services and activities conducted by ICS-CERT, visit http://ics-cert.us-cert.gov/.

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-13-016-02, Siemens S7 Password Offline Brute-force Tool, (January 16, 2013)

ICS-Alert-13-016-01, Schneider Electric Products, (January 16, 2013)

ICS-Alert-13-009-01, Advantech WebAccess, (January 09, 2013)

ICS-Alert-13-004-01, Advantech Studio Web Server, (January 04, 2013)

ADVISORIES

ICSA-13-053-02 – Honeywell Enterprise Buildings Integrator (EBI) SymmetrE and ComfortPoint Open Manager Station, (February 22, 2013)

ICSA-13-036-01A – (UPDATE) Wonderware Intelligence Tableau Server Ruby on Rails Improper Input Validation, (February 21, 2013)

ICSA-13-050-01 – 3S CODESYS Gateway-Server Multiple Vulnerabilities, (February 19, 2013)

ICSA-13-045-01 – Tridium NiagaraAX Directory Traversal Vulnerability, (February 14, 2013)

ICSA-13-043-02 – WellinTech KingView KingMess Buffer Overflow, (February 12, 2013)

ICSA-13-043-01 – Schneider Electric Accutech Manager Heap Overflow, (February 12, 2013)

ICSA-13-042-01 – MOXA EDR-G903 Series Vulnerabilities, (February 11, 2013)

ICSA-13-036-02 – Ecava IntegraXor ActiveX Buffer Overflow, (February 05, 2013)

ICSA-13-024-01, – Beijer Electronics ADP and H-Designer Buffer Overflow Vulnerability, (January 24, 2013)

ICSA-13-022-02, – GE Intelligent Platforms Proficy Cimplicity Multiple Vulnerabilities, (January 22, 2013)

ICSA-13-022-01, – GE Proficy Real-Time Information Portal Information Disclosure Vulnerabilities, (January 22, 2013)

ICSA-13-018-01, – Schneider Electric IGSS Buffer Overflow, (January 18, 2013)

ICSA-13-016-01, – Schnieder Electric Authenticated Communication Risk Vulnerability, (January 16, 2013)

ICSA-13-014-01, – Siemens SIMATIC RF Manager ActiveX Buffer Overflow, (January 14, 2013)

ICSA-13-011-03, – Rockwell Automation ControlLogix Multiple PLC Vulnerabilities, (January 11, 2013)

ICSA-13-011-02, – SpecView Directory Traversal, (January 11, 2013)

ICSA-13-011-01, – 3S CoDeSys Multiple Vulnerabilities, (January 11, 2013)

ICSA-12-362-01, – iGen opLYNX Central Authentication Bypass (December 27, 2012)

ICSA-12-354-02, – Carlo Gavazzi EOS-Box Multiple Vulnerabilities (December 19, 2012)

ICSA-12-354-01, – RuggedCom ROS Hard-Coded RSA SSL Private Key (December 19, 2012)

ICSA-12-342-01A, – (UPDATE) Rockwell Allen-Bradley MicroLogix (December 11, 2012)

ICSA-12-297-01, – Tropos Wireless Mesh Routers Insufficient Entropy Vulnerability (December 10, 2012)

OTHER

The ICS-CERT Monitor October/November/December 2012 issue summarizes highlights of ICS-CERT activities from the last quarter 2012.

Follow ICS-CERT on Twitter: @icscert

NOTEWORTHY NEWS HIGHLIGHTS

Napolitano Addresses the Future Goals of DHS, Sequestration Cuts
2013-02-26

At a Brookings Institution event on Tuesday, Feb. 26, Homeland Security Secretary Janet Napolitano acknowledged the upcoming 10th anniversary of the DHS next month by outlining the progress of the organization and goals for the future. Citing aviation security, cybersecurity, border security and the ability to respond to disasters from all hazards, Napolitano said it's important to continue developing risk-based strategies, and to continue to foster collaboration between the public and private sectors to facilitate information sharing. On cybersecurity, she said a top priority is to develop "a 21st-century cyber workforce, the next generation of skilled individuals who want to come to DHS, make an impact and serve their country in this field." She also said it is imperative that the public and private sectors work together more effectively by sharing information and promoting adoption of cybersecurity best practices. "We need greater information sharing so that the government can learn from the private sector where people fight this every day," she said. "And we need to ensure that the government can use information at various levels of classification to help the private sector itself."

http://www.emergencymgmt.com/safety/Napolitano-Addresses-Future-Goals-DHS html

DHS Cybersecurity Boss Pushes 'Cyber 911', New Voluntary Standards
2013-02-25

One of the federal government's top cybersecurity officials has big plans for shoring up the nation's information security posture, including formalizing a "cyberattack 911" service and creating a new set of voluntary security standards for private companies. Mark Weatherford, deputy under secretary for cybersecurity at the Department of Homeland Security (DHS), used his opening keynote at the Cloud Security Alliance Summit 2013, a precursor to the 2013 RSA Conference, to outline his strategy for using the capabilities and influence of DHS to improve national cybersecurity, particularly for organizations that manage critical infrastructure. Weatherford said his group's four major responsibilities are: to oversee cybersecurity at federal civilian agencies; provide infosec support and best practices to critical infrastructure firms; coordinate cybersecurity attack response for major incidents in the private sector (like the recent distributed denial-of-service attacks against several financial companies); and engage in cybersecurity diplomacy and policymaking nationally and internationally. Weatherford said one of the challenges he's faced in the 15 months he's been at DHS is that private sector organizations often don't know who to contact when they need urgent cybersecurity support from the government. However, he said that's about to change. In part to support that goal, Weatherford said he reorganized his group within DHS into several teams with specific responsibilities, one of which is offering urgent support and ongoing outreach across the nation, especially to state and local governments, educating them about the cybersecurity resources available to them via DHS.

http://searchsecurity.techtarget.com/news/2240178574/DHS-cybersecurity-boss-pushes-cyber-911-new-voluntary-standards

Hacking Victim Bit9 Blames SQL Injection Flaw
2013-02-25

Bit9 said a common Web application vulnerability was responsible for allowing hackers to ironically use the security vendor's systems as a launch pad for attacks on other organizations. Based in Waltham, Massachusetts, the company sells a security platform that is designed in part to stop hackers from installing their own malicious software. In an embarrassing admission, Bit9 said earlier this month that it neglected to install its own software on a part of its network, which lead to the compromise. In a more detailed explanation on its blog on Monday, Bit9 said attackers gained access by exploiting a SQL injection flaw in one of its Internet-facing Web servers. A SQL injection flaw can allow a hacker to enter commands into a web-based form and get the backend database to respond. The compromise happened around July 2012, wrote Bit9's CTO Harry Sverdlove. Once inside Bit9, the hackers accessed a virtual machine used to digitally sign code for Bit9, a security measure that verifies the company's code is legitimate. The compromised server was shut down for about six months, but was brought back online in January. Bit9 then discovered the problem. "We took immediate containment and remediation steps, revoked the certificate in question and reached out to our entire customer base," Sverdlove wrote.

The hackers used Bit9's certificate to sign 32 of their own malicious files and scripts. Sverdlove described some of the malware as backdoors with the names "HiKit" and "HomeUNIX."

http://www.cio.com/article/729401/Hacking_Victim_Bit9_Blames_SQL_Injection_Flaw?taxonomyId=3089

Chinese Army Unit Is Seen as Tied to Hacking Against U.S.
2013-02-18

An unusually detailed 60-page study, to be released Tuesday by Mandiant, an American computer security firm, tracks for the first time individual members of the most sophisticated of the Chinese hacking groups — known to many of its victims in the

NOTEWORTHY NEWS HIGHLIGHTS - Continued

United States as "Comment Crew" or "Shanghai Group" — to the doorstep of the military unit's headquarters. The firm was not able to place the hackers inside the 12-story building, but makes a case there is no other plausible explanation for why so many attacks come out of one comparatively small area.

http://www nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us html

http://intelreport mandiant.com/Mandiant_APT1_Report.pdf

A Chinese Hacker's Identity Unmasked
2013-02-14

Up to now, private-sector researchers such as Stewart have had scant success putting faces to the hacks. There have been faint clues left behind—aliases used in domain registrations, old online profiles, or posts on discussion boards that give the odd glimpse of hackers at work—but rarely an identity. Occasionally, though, hackers mess up. Recently, one hacker's mistakes led a reporter right to his door.

http://www.businessweek.com/articles/2013-02-14/a-chinese-hackers-identity-unmasked

Presidential Policy Directive -- Critical Infrastructure Security and Resilience
2013-02-12

Critical Infrastructure Security and Resilience The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

SCADA, ICS Bug Brokering Mirrors IT Vulnerability Market
2013-02-05

The world of SCADA and industrial control system vulnerabilities is starting to mirror that of IT security, not only in the demonstration and exploitation of zero-day vulnerabilities, but in the brokering of flaws and exploits between hackers and organizations interested in buying research.

Today at the Kaspersky Security Analyst Summit, two researchers known for finding more than 1,000 vulnerabilities in Internet-facing industrial control systems, demonstrated a zero-day in vendor Tridium's Niagara Framework, which is used to run building maintenance systems including elevators, HVAC, video surveillance systems and more.

The vulnerability was reported by Cylance researchers Billy Rios and Terry McCorkle in January 2012 and has yet to be patched; Rios and McCorkle said they've been working with Tridium, which acknowledged the flaw in April. Tridium, the researchers said, is expected to release a fix soon.

https://threatpost.com/en_us/blogs/scada-ics-bug-brokering-mirrors-it-vulnerability-market-020513

Zeus Source Code Leaked
2013-02-04

Back in February, the infamous Zeus Trojan source code was known to be made available on underground hacking and tools forums. At that time the cost of the code was around $100,000. Several weeks later, the price was just $5000. Now it's available for free.

http://blog.spamfighter.com/malware-2/zeus-source-code-leaked.html

Oracle Issues Emergency Java Security Update
2013-02-04

Oracle's Java update addresses 50 bugs, including flaws that can be used to remotely compromise a desktop or server.

http://www.informationweek.com/security/vulnerabilities/oracle-issues-emergency-java-security-up/240147724

Broad Powers Seen for Obama in Cyberstrikes
2013-02-03

A secret legal review on the use of America's growing arsenal of cyberweapons has concluded that President Obama has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad, according to officials involved in the review.

That decision is among several reached in recent months as the administration moves, in the next few weeks, to approve the nation's first rules for how the military can defend, or retaliate, against a major cyberattack. New policies will also govern how the intelligence agencies can carry out searches of faraway computer networks for signs of potential attacks on the United States and, if the president approves, attack adversaries by injecting them with destructive code — even if there is no declared war.

http://www nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html

NOTEWORTHY NEWS HIGHLIGHTS - Continued

Year One in global cyber war
2012-12-15

As cyberattacks mounted in 2012, the DOD and other government agencies began striking back, "We're seeing cyber conflict every single day," said Anup Ghosh, a former Defense Advanced Research Projects Agency (DARPA) senior scientist and program manager. "We're seeing the wholesale compromise of our nation's networks across all industries and the government," said Ghosh, who is now CEO and founder of Invincea, a security software developer located in Fairfax, Va.

"There's no one who is immune to nation-state attacks, and we have to face it from all different types of nations," Ghosh said. In a certain sense, cyber creates a level playing field, he observed. "A level playing field between so-called Third World countries with limited military capabilities to our cyber capabilities."

http://defensesystems.com/articles/2012/11/15/cyber-defense-year-in-review.aspx

How to bring down mission-critical GPS networks with $2,500
2012-12-14

Scientists have devised a series of novel and inexpensive attacks that can severely disrupt mission-critical global positioning systems relied on by the military and a variety of industrial players, including airlines, mining companies, and operators of hydroelectric plants and other critical infrastructure.

Unlike previous GPS attacks, the one developed by a team of scientists from Carnegie Mellon University and a private navigation company exploits software bugs in the underlying receivers. That allows the attacks to be stealthier and more persistent than earlier exploits, which primarily relied on signal jamming and spoofing. Prototype hardware that cost only $2,500 to build is able to cause a wide variety of GPS devices within a 30 mile radius to malfunction. Because many of those devices are nodes on special networks that make GPS signals more precise, the attacks have the effect of disrupting larger systems used in aviation, military, and critical infrastructure.

http://arstechnica.com/security/2012/12/how-to-bring-down-mission-critical-gps-networks-with-2500/

Skynet, the potential use of Tor as a bulletproof botnet
2012-12-11

In September 2012 the German security firm G Data Software detected a botnet with a particular feature, it is controlled from an Internet Relay Chat (IRC) server running as a hidden service of the Tor.

http://www.infosecisland.com/blogview/22779-Skynet-the-potential-use-of-Tor-as-a-bulletproof-botnet html

"Dexter" malware steals credit card data from point-of-sale terminals
2012-12-11

A researcher has uncovered new malware that steals payment card data from point-of-sale terminals used by stores, hotels, and other businesses.

Dexter, as the malware is called, has infected hundreds of point-of-sale computers at big-name retailers, hotels, restaurants, and other businesses, according to a report issued by Aviv Raff, chief technology officer of Israel-based security firm Seculert. Businesses infected in the past three months are located in 40 different countries, with 30 percent of those compromised located in the US, 19 percent in the UK, and nine percent in Canada. Malware that infects point-of-sale terminals can be one of the most efficient ways to carry out payment card fraud because it targets machines with access to large amounts of the required data.

http://arstechnica.com/security/2012/12/dexter-malware-steals-credit-card-data-from-point-of-sale-terminals/

Aramco Says Cyberattack Was Aimed At Production
2012-12-09

Saudi Arabia's national oil company, Aramco, said on Sunday that a cyberattack against it in August that damaged some 30,000 computers was aimed at stopping oil and gas production in Saudi Arabia, the biggest exporter in the Organization of the Petroleum Exporting Countries. The attack on Saudi Aramco — which supplies a tenth of the world's oil — failed to disrupt production, but was one of the most destructive hacker strikes against a single business. "The main target in this attack was to stop the flow of oil and gas to local and international markets and thank God they were not able to achieve their goals," Abdullah al-Saadan, Aramco's vice president for corporate planning, said on Al Ekhbariya television. It was Aramco's first comments on the apparent aim of the attack.

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

UK Officials: Our Critical Infrastructure Has Already Been Hit by Cyberattacks
2012-12-04

United Kingdom officials have admitted that the country's most critical infrastructures have already been attacked by hostile foreign states.

NOTEWORTHY NEWS HIGHLIGHTS - Continued

http://news.softpedia.com/news/UK-Officials-Our-Critical-Infrastructure-Has-Already-Been-Hit-by-Cyberattacks-311908.shtml

Utilities' Cyber Survey May be Model for Other Industries 2012-12-04

A White House effort to improve the cybersecurity of the nation's commercial power grid could soon be expanded to other critical sectors, such as transportation and water. The Energy and Homeland Security departments kicked off the initiative, known as the Electricity Sector Cybersecurity Capability Maturity Model, this year as an effort to assess and improve the security of thousands of utility companies. A key component of the initiative is a self-evaluation survey of more than 300 questions that helps utilities evaluate their cybersecurity, identify gaps and plan how to mitigate risks and implement necessary changes.

http://www federaltimes.com/article/20121204/IT01/312040006/

Vulnerabilities Threaten to Crash MySQL Databases 2012-12-03

A number of vulnerabilities have been discovered in the popular database software MySQL that could allow attackers to crash the service and deny access to users.

http://www.zdnet.com/vulnerabilities-threaten-to-crash-mysql-databases-7000008194/

UPCOMING EVENTS 2013

March

CANCELLED*

Houston Regional Training (4 days)
March 26–29, 2013
The Woodland Town Center
Houston, TX
Course Description and Registration

May

CANCELLED*

ICSJWG Introduction to Control Systems Cybersecurity Training (1 day)
May 2, 2013
Phoenix, AZ
Course Description and Registration

CANCELLED*

Industrial Control Systems Cybersecurity Joint Working Group (ICSJWG) 2013 Spring Conference (4 day)
May 6–9, 2013
Phoenix, AZ
Course Description and Registration

June

Industrial Control Systems Cybersecurity (301) Training (5 days) North American Partners
June 17–21, 2013
Idaho Falls, ID
Course Description and Registration

CANCELLED*

Cybersecurity Training for Industrial Control Systems (4 days)
June 24–27, 2013
Boston, MA
Course Description and Registration

* Due to Sequestration, these events have been cancelled. We apologize for the inconvenience. If you have questions, contact us at cssp_training@hq.dhs.gov.

COORDINATED VULNERABILITY DISCLOSURE

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

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

RESEARCHERS ASSISTING ICS-CERT IN DEC, JAN, AND FEB

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

- Juan Vazquez of Rapid7, ICSA-13-053-02 – Honeywell Enterprise Buildings Integrator (EBI) SymmetrE and ComfortPoint Open Manager Station, (February 22, 2013).
- Aaron Patterson, ICSA-13-036-01A` – (UPDATE) Wonderware Intelligence Tableau Server Ruby on Rails Improper Input Validation, (February 21, 2013)
- Aaron Portnoy of Exodus Intelligence, ICSA-13-050-01 – 3S CODESYS Gateway-Server Multiple Vulnerabilities, (February 19, 2013)
- Billy Rios and Terry McCorkle, ICSA-13-045-01 – Tridium NiagaraAX Directory Traversal Vulnerability, (February 14, 2013)
- Lucas Apa and Carlos Mario Penagos Hollman of IOActive, ICSA-13-043-02 – WellinTech KingView KingMess Buffer Overflow, (February 12, 2013)
- Aaron Portnoy of Exodus Intelligence, ICSA-13-043-01 – Schneider Electric Accutech Manager Heap Overflow, (February 12, 2013)
- Neil Smith, ICSA-13-042-01 – MOXA EDR-G903 Series Vulnerabilities, (February 11, 2013)
- Andrew Brooks, ICSA-13-036-02 – Ecava IntegraXor ActiveX Buffer Overflow, (February 05, 2013)
- Kuang-Chun Hung of Information and Communication Security Technology Center (ICST), ICSA-13-024-01 - Beijer Electronics ADP and H-Designer Buffer Overflow Vulnerability, (January 24, 2013).
- General Electric self-reported, ICSA-13-022-02 - GE Intelligent Platforms Proficy Cimplicity Multiple Vulnerabilities, (January 22, 2013).
- General Electric self-reported, ICSA-13-022-01 - GE Proficy Real-Time Information Portal Information Disclosure Vulnerabilities, (January 22, 2013).
- Aaron Portnoy of Exodus Intelligence, ICSA-13-018-01 - Schneider Electric IGSS Buffer Overflow, (January 18, 2013).
- Schneider Electric self-reported, ICSA-13-016-01 - Schneider Electric Authenticated Communication Risk Vulnerability, (January 16, 2013).
- Siemens self-reported, ICSA-13-014-01 - Siemens SIMATIC RF Manager ActiveX Buffer Overflow, (January 14, 2013).
- Rubén Santamarta of IOActive, ICSA-13-011-03 - Rockwell Automation ControlLogix Multiple PLC Vulnerabilities, (January 11, 2013).
- Independent researcher Luigi Auriemma, ICSA-13-011-02 - SpecView Directory Traversal, (January 11, 2013).
- Reid Wightman of IOActive, ICSA-13-011-01 - 3S CoDeSys Multiple Vulnerabilities, (January 11, 2013)
- Independent researcher Anthony Cicalla, ICSA-12-362-01 - iGen opLYNX Central Authentication Bypass (December 27, 2012).
- Carlo Gavazzi self-reported, ICSA-12-354-02 - Carlo Gavazzi EOS-Box Multiple Vulnerabilities (December 19, 2012).

DOCUMENT FAQ

What is the publication schedule for this digest?

ICS-CERT publishes the ICS-CERT Monitor when an adequate amount of pertinent information has been collected..

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

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

COORDINATED VULNERABILITY DISCLOSURE - Continued

- Justin W. Clarke of Cylance Inc, ICSA-12-354-01 - RuggedCom ROS Hard-Coded RSA SSL Private Key (December 19, 2012).
- Matthew Luallen of CYBALTI, ICSA-12-342-01A - (UPDATE) Rockwell Allen-Bradley MicroLogix (December 11, 2012). An independent research group composed of Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, ICSA-12-297-01-Tropos Wireless Mesh Routers Insufficient Entropy Vulnerability (December 10, 2012).
- An independent research group composed of Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, ICSA-12-297-01-Tropos Wireless Mesh Routers Insufficient Entropy Vulnerability (December 10, 2012).

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2012

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

Aaron Patterson
Aaron Portnoy
Andrew Brooks
Anton Popov
Arthur Gervais
Billy Rios
Bob Radvanovsky
Brendan Harris
Carlos Mario Penagos Hollmann
Carsten Eiram
Cesar Cerrudo
Dale Peterson
Dillion Beresford
Nadia Heninger
Eric Wustrow
J. Alex Halderman
Joel Langill
Jon Christmas
Juan Vasquez
Kuang-Chun Hung (ICST)
Lucas Apa
Luigi Auriemma
Michael Toecker
Neil Smith
Postive Technologies Security
Reid Wightman
Rubén Santamarta
Sergey Gordeychick
Shawn Merdinger
Terry McCorkle
Zakir Durumeric

We Want To Hear From You

A key aspect of our mission is providing relevant and timely cybersecurity information products and services to industrial control system (ICS) stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we can work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to: ics-cert@hq.dhs.gov.