ICS-CERT MONTHLY MONITOR

NOVEMBER 2011

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

CYBER TIP

While antivirus, intrusion prevention and detection software, and properly configured and tested firewalls provide a base layer of protection, having a knowledge and understanding of operational data traffic is also important. Real time file and directory monitoring can provide a highly effective level of protection. Tools that monitor normally static files and directory trees for unexpected changes are an important detection indicator for possible malicious activity. These capabilities should be deployed on software servers, intellectual property repositories and network traffic nodes. Archives of system directories and files, networks, system and software configuration files before every authorized configuration changes are important, if needed for recovery.

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 and 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.

VULNERABILITY DISCLOSURE

ICSJWG Industrial Control Systems Vulnerabililty Disclosure Panel

The ICS-CERT participated in a panel titled ***Industrial Control System Vulnerability Disclosure*** at the Industrial Control Systems Joint Working Group (ICSJWG) 2011 Fall Conference held October 24-27 in Long Beach, CA. The purpose of the panel was to foster open dialog about control systems vulnerabilities and how the community can work together to mitigate these difficult issues.

Eric Cornelius, DHS ICS-CERT Technical Lead, moderated the panel that included Dale Peterson, founder and CEO of Digital Bond, Inc; Ernest Rakaczky, IOM Portfolio Program Manager for Control Systems Cyber Security at Invensys; Lieutenant Colonel Andrew Pennington, US Air Force Reserves and Senior Program Manager for Cyber Security Training at K2Share, LLC; and Kevin Hemsley, Lead Vulnerability Handler for ICS-CERT.

Kevin Hemsley discussed the increased number of ICS-related vulnerabilities over the past year (up 753% for ICS-CERT) and the affect that this trend has had on the community. He affirmed the sharp increase has underscored the importance of a more strategic and calculated approach in order to prioritize those that are more severe in nature. Mr. Peterson emphasized this stating that ICS-CERT must focus on analyzing the vulnerabilities that have the potential for having large impacts on critical infrastructure. Also along these lines, Mr. Rakaczky noted that the ICS community as a whole needs to further develop collaborative mitigations to these and other difficult issues impacting ICS security.

Another hot-button topic had to do with vulnerability disclosure. Mr. Peterson stated that it is the responsibility of ICS-CERT to provide an effective means to get vulnerability information out to ICS users and support organizations that vendors may not be able to easily reach. While Mr. Peterson indicated ICS-CERT is doing well in this area, he believes

(continues on page 2)

NCCIC NEWS

Weatherford Appointed Deputy Under Secretary for Cybersecurity

DHS has announced the appointment of Mark Weatherford as the new Deputy Under Secretary for Cybersecurity for the National Protection and Programs Directorate (NPPD), a newly created position that will allow DHS to better carry out its mission to create a safe, secure, and resilient cyberspace.

Mr. Weatherford brings a welcomed wealth of experience and knowledge to the Department in the area of cybersecurity and critical infrastructure and key resources. He previously served as Vice President and Chief Security Officer at the North American Electric Reliability Corporation (NERC), where he directed the organization's critical infrastructure and cybersecurity program. In addition, he served as Chief Information Security Officer in the State of California's Office of Information Security, and as Chief Security Officer for the State of Colorado, where he helped establish the state's first cybersecurity program. Prior to that, Mr. Weatherford led the Navy's Computer Network Defense operations and the Naval Computer Incident Response Team.

ANNOUNCEMENTS

Control Systems Security Program Releases FY 2011 Year in Review

The Control Systems Security Program (CSSP) has released its FY 2011 Year in Review. This document highlights the many accomplishments of both the CSSP and its operational component, the ICS-CERT. The document can be found at:

http://www.us-cert.gov/control_systems/pdf/Year_in_Review_FY2011_Final.pdf

NESCO Joins the NCCIC

The National Electric Sector Cybersecurity Organization (NESCO) operated by EnergySec, has signed a formal Cooperative Research and Development Agreement (CRADA) with the Department of Homeland Security (DHS) to share information with the National Cybersecurity and Communications Integration Center (NCCIC). This agreement will foster greater information sharing and collaboration between the two organizations to better serve the electric sector in warding off cyber attacks.

VULNERABILITY DISCLOSURE

(vulnerability disclosure continued from page 1)

that in many instances there can be improvement in the level and clarity of information provided. Kevin Hemsley agreed that improvements can be made to ICS-CERT information products. He stated that as ICS-CERT matures, it continuously strives to improve its processes and procedures, and he invited direct feedback from the community.

Also during the panel, the topic of ICS-CERT's researcher attribution policy was discussed. Prior to the discussion, researchers who did not coordinate with the vendor, ICS-CERT, or other coordinating entities were not attributed in ICS-CERT products. Based on feedback received at this panel and from other sources, ICS-CERT has revisited and revised its policy on researcher attribution. Changes to this policy are discussed in the ["Changes to ICS-CERT Researcher Attribution Policy"] section below.

ICS-CERT enjoyed the opportunity to participate in this panel as well as the constructive feedback that it generated. ICS-CERT looks forward to continued open and honest discussions in order to further evaluate the best approaches and policies for better serving the control systems community.

Changes to ICS-CERT's Researcher Attribution Policy

As referenced in the article "ICSJWG Industrial Control System Vulnerability Disclosure Panel" on page 1, ICS-CERT received numerous requests to revisit the existing policy to only provide attribution (researcher's names) when coordinated disclosure occurred. Much of the feedback requested that attribution be made in our alerts and advisories regardless of whether vulnerabilities were previously coordinated. Many felt that this would enable them to more easily identify additional sources of information related to vulnerabilities.

Well, you've spoken and we've listened. ICS-CERT will begin providing attribution to researchers in products such as alerts and advisories regardless of coordination. (Researchers who wish to remain anonymous will not be named upon request.) It is ICS-CERT's belief that this policy change will foster stronger relationships between vendors and researchers, which will ultimately benefit the owner/ operator community at large.

ICS-CERT continues to strongly recommend that researchers coordinate with the vendor, ICS-CERT, or other coordination entities prior to disclosure of vulnerability details. This coordination will allow vendors time to develop and test mitigations, and asset owners to be provided with information and mitigation options prior to a public disclosure of the vulnerability.

Internet Facing Systems

ICS-CERT recently responded to reports by an independent security researcher, Eireann Leverett, who used the SHODAN search engine to discover thousands of Internet facing control system devices throughout the world as part of his Master's thesis research at Cambridge University. Some of these Internet facing systems could be using potentially insecure mechanisms for authentication, including default username and password, and could be susceptible to known or 0-day vulnerabilities. The identified systems span several critical infrastructure sectors and vary in their deployment footprints. Mr. Leverett has coordinated his findings with ICS-CERT, and ICS-CERT has been working to reduce the risk to critical infrastructure and key resource owners and operators by coordinating directly with over 60 CERTS worldwide to assist with mitigation. ICS-CERT plans to start coordinating with identified vendors soon.

ICS-CERT has recently responded to similar issues involving Internet facing control system devices.

- In April of this year, ICS-CERT responded to reports of over 70 instances of Internet facing control system devices, mostly in the water sector.
- In October, ICS-CERT responded to an incident involving Internet facing electrical substations.

ICS owners and operators often use Internet accessible systems for remote access to monitor system status or management certain features. However, if remote access is not properly configured and carefully managed, these systems are at increased risk for cyber attacks and intrusions.

ICS-CERT continues to recommend that owners and operators minimize control system exposure to the Internet by locating control system networks and remote devices behind properly configured and tested firewalls, and by implementing more secure means of remote access, such as virtual private network (VPN). For additional information, please review the ICS-CERT alert discussing the risks associated with Internet facing controls system devices. This alert provides a more complete description of the risks and associated mitigations and suggestions for protecting control systems that require Internet access . The alert can be downloaded from the following location: http://www.uscert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf.

DUQU Update

In mid-October, the industrial control system community became aware of new malware that had been found in the wild. Initial reports indicated that this malware, named Duqu, was intended to target and acquire information from specific organizations, possibly including industrial control systems (ICS) manufacturers. In reaction to the report of a targeted information acquisition threat against industrial control systems manufacturers, ICS-CERT and US-CERT engaged with the sources of various reports and the original researchers, Hungarian-based CrySyS (Laboratory of Cryptography and System Security) to assist with the malware analysis.

ICS-CERT and US-CERT analysis of multiple variants of Duqu, as well as findings from CrySyS and several security vendors (including Symantec, McAfee, Kaspersky Labs and SecureWorks) yielded no evidence that Duqu targeted owners, operators, vendors, or ICS manufacturers. In addition, few infected organizations have been identified to date. Of the organizations believed to be infected, Symantec reports only six, located in France, Netherlands, Switzerland, Ukraine, India, Iran, Sudan, and Vietnam. Other security vendors have indicated that organizations in Austria, Hungary, Indonesia, and United Kingdom may also be infected.

Current understanding is that Duqu is a remote access Trojan (RAT) intended to collect and exfiltrate network, keystroke and other system information. Duqu executes data exfiltration using image files (.jpg) in an attempt to disguise the stolen data as normal benign network traffic. To date, one Duqu dropper has been identified that exploits a previously unknown (0-day) Windows kernel vulnerability. Once on a system, the infection can spread to other networked systems and can form a peer-to-peer command and control (C&C) protocol. This minimizes the detection footprint to only the original infected system. Multiple Duqu variants have been identified, each having its own signature and C&C server, making it difficult for antivirus software to detect new infections.

Duqu's modularity indicates it is primarily a delivery system that can be combined with any number of malware payloads. Recent reports now show that Duqu has used at least two separate infostealer tools.

Initial reports associated Duqu with Stuxnet, which increased the interest in Duqu within the ICS community. Specifically, several reports were published concerning the similarities in the code for the two malwares and the possibility that they originated from the same author. However, ICS-CERT and US-CERT analysis of the code and each malware's characteristics indicates significant differences between Duqu and Stuxnet, lending more fuel to the debate about common authorship. Some of the major differences are:

- Stuxnet was self-replicating while Duqu is not.
- Duqu uses a dropper that exploits a previously unknown (0-day) Windows kernel vulnerability using a specially crafted Microsoft Word document. Stuxnet exploited multiple previously unknown (0-day) vulnerabilities and used various methods (USB drives, project files and other) to propagate the infection.
- Stuxnet and Duqu appear to be designed for completely different purposes. Stuxnet was apparently crafted to target a specific ICS configuration, while Duqu appears to exfiltrate system, network, and user information to multiple C&C servers.

To date, ICS-CERT has released a series of six alerts and updates titled "ICS-ALERT-11-291-01-W32.Duqu: An Information-Gathering Malware." The most recent information released by ICS-CERT regarding Duqu can be found in the Joint Security Awareness Report, JSAR-11-312-01-W32.DUQU-MALWARE, published by ICS-CERT and US-CERT on the ICS-CERT web page. ICS-CERT and US-CERT will continue to analyze Duqu and other threats to CIKR and report as appropriate.

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-11-291-01D - (UPDATE) W32 Duqu-Malware"

Update D consists of four informational updates. This updated Alert is a follow-up to the Alert titled "ICS-ALERT-11-291-01CP-W.32 Duqu:An Information Gathering Malware Targeting ICS Manufacturers" (containing FOUO-related content) released on the US-CERT Secure Portal. This update mentions the Kaspersky Labs "The Mystery of Duqu: Part Two," additional indicator files, and updated information concerning known new variants of Duqu.

Alert "ICS-ALERT-11-291-01B - (UPDATE) W32.Duqu: An Information Gathering Malware Targeting ICS Manufacturers"

This alert updates the previous alert update titled "ICS-ALERT-11-291-01A - W32 Duqu-Malware Targeting ICS Manufacturers" that was published October 20, 2011, on the ICS-CERT web with one update. ICS-CERT, in close coordination with Symantec and the original researchers, has determined after additional analysis that neither industrial control systems nor vendors/manufacturers were targeted by Duqu.

Alert "ICS-ALERT-11-291-01A - (UPDATE) W32.Duqu: An Information Gathering Malware Targeting ICS Manufacturers"

This alert is an update to the original alert posted on the website October 18, 2011. This update contained two updates to the original alert: 1) identification of a command and control server and 2) encouragement to organizations to update antivirus definitions, as Duqu definitions are available on the major antivirus sites.

Alert "ICS-ALERT-11-291-01 - W32. Duqu: An Information Gathering Malware Targeting ICS Manufacturers"

On October 18, 2011, Symantec released a Security Response Report (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf) describing W32.Duqu, an information gathering threat targeting specific organizations, including industrial control system manufacturers. According to Symantec, W32.Duqu does not contain any code related to industrial control systems (ICS) and is primarily a remote access Trojan (RAT).

Alert "ICS-ALERT-11-286-01 - Microsys SPOL sr.o Promotic"

ICS-CERT is aware of a public report of three vulnerabilities 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. 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-11-285-01 - Open Automation Software OPC Systems.Net"

This alert supersedes ICS-ALERT-11-283-03-OPC Systems.

ICS-CERT is aware of a public report of a vulnerability with proof-of-concept (PoC) exploit code affecting Open Automation Software's OPC Systems.Net product. OPC Systems.Net is a supervisory control and data acquisition/human machine interface (SCADA/HMI) product. According to this report, the vulnerability is exploitable through a malformed .NET Remote Procedural Call (RPC) packet.

Alert "ICS-ALERT-11-283-02 - ATVISE WebMI Multiple Vulnerabilities"

ICS-CERT is aware of a public report of four vulnerabilities with proof-of-concept (PoC) exploit code affecting atvise webMI, a web-based SCADA/HMI product. According to this report, these vulnerabilities are remotely exploitable through webserver Port 80/TCP. This report was released without coordination with either the vendor or ICS-CERT.

Alert "ICS-ALERT-11-283-01 - IRAI AUTOMGEN Buffer Overflow"

ICS-CERT is aware of a public report of a buffer overflow vulnerability with potential code execution affecting IRAI Automgen, a HMI/SCADA product. According to this report, the vulnerability is exploitable by running a malformed project file.

ADVISORIES

Advisory "ICSA-11-294-01 - Progea Movicon Power HMI Vulnerabilities"

This advisory is a follow-up to the Alert titled "ICS-ALERT-11-256-01 - Multiple Vulnerabilities in Progea Movicon" that was published September 13, 2011, on the ICS-CERT web page. Two buffer overflow and one memory corruption vulnerability were disclosed affecting the Progea Movicon's PowerHMI product.

Advisory "ICSA-11-277-01 - Schneider Electric UnitelWay Buffer Overflow"

ICS-CERT originally released Advisory ICSA-11-277-01P on the US-CERT secure Portal on October 04, 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 Technology Center (ICST) has identified a buffer overflow vulnerability in UnitelWay Windows Device Driver. This device driver is deployed as part of several different Schneider Electric products.

Advisory "ICSA-11-285-01 - Honeywell TEMA remote installer activeX vulnerability"

ICS-CERT received a report from independent security researchers Billy Rios and Terry McCorkle concerning a vulnerability affecting Honeywell Enterprise Buildings Integrator (EBI) software systems that have Temaline products installed. Temaline software products use the Tema Remote Installer to download and install required Tema components.

RECENT PRODUCT RELEASES

Advisory "ICSA-11-279-03A - Unitronics UniOPC Server Input handling Vulnerability"

Independent security researchers Billy Rios and Terry McCorkle have identified a vulnerability in Unitronics' UniOPC Server product. This update includes three updates identifying that this vulnerability is a result of improper handling of input by a third-party component, https50.ocx, which is part of "IP*Works! SSL."

Advisory "ICSA-11-279-03 - Unitronics UniOPC Server Input Handling Vulnerability"

Security researchers Billy Rios and Terry McCorkle have identified a vulnerability in Unitronics UniOPC Server product. This vulnerability is a result of the improper handling of input by a third-party component, "IP*Works! SSL," which is used in the UniOPC product. Successful exploitation of this vulnerability results in a crash and could result in the execution of arbitrary code.

Advisory "ICSA-11-280-01 - Cogent DataHub Multiple Vulnerabilities"

This Advisory is a follow-up to the Alert, "ICS-ALERT-11-256-03 - COGENT DATAHUB MULTIPLE VULNERABILITIES," that was published September 13, 2011, on the ICS-CERT web page.

ICS-CERT is aware of a public report of multiple vulnerabilities in Cogent's DataHub application. These vulnerabilities include denial of service, information leakage, and remote code execution. Cogent has produced a patch that resolves these vulnerabilities in DataHub. ICS-CERT has not tested this patch to validate that it resolves this vulnerability.

Advisory "ICSA-11-273-03A - Rockwell RSLogix Denial-of-Service Vulnerability "

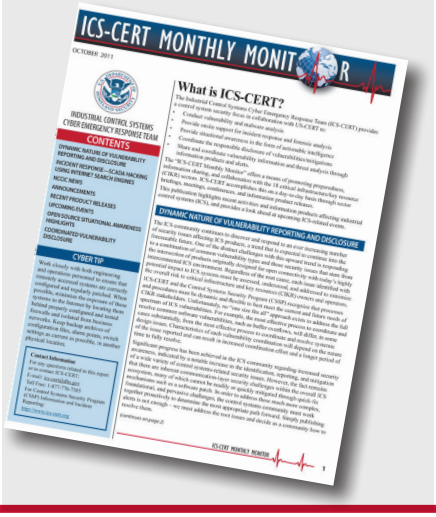
This updated Advisory is a follow-up to the original Advisory titled "ICSA-11-273-03—Rockwell RSLogix Denial-of-Service Vulnerability" that was published September 30, 2011, on the ICS-CERT web page.

Advisory "ICSA-11-279-04 - Beckoff TwinCAT"

This Advisory is a follow-up to the Alert, "ICS-ALERT-11-256-06 - BECKHOFF TWINCAT DENIAL-OF-SERVICE VULNERABILITY," that was published September 13, 2011, on the ICS-CERT web page. ICS-CERT is aware of a public report of a denial-of-service vulnerability as a result of a read access violation in Beckhoff's TwinCAT Software. Beckhoff has produced a patch to address this vulnerability in TwinCAT Software.

OTHER

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



UPCOMING EVENTS

NOVEMBER

2011 TSA Cyber Security in Transportation Summit

November 1–2, 2011

Sheraton Crystal City

Arlington, VA 22202

Registration: https://www.signup4 net/public/ap.aspx?EID=TSAC10E&OID=130

Contact:
cybersecurity @tsa.dhs.gov

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)

November 7−11, 2011

Control Systems Analysis Center

Idaho Falls, ID 83415

Registration

DECEMBER

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)

December 5−9, 2011

Control Systems Analysis Center

Idaho Falls, ID 83415

Registration

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.

Report: French Nuclear Company Areva Hit by Virus

2011-10-31

"French nuclear power group Areva was the target of a cyber attack in September, according to a recent post on the website of French business magazine L'Expansion."

http://threatpost.com/en_us/blogs/french-nuclear-company-areva-hit-virus-103111

'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

The Mystery of Duqu: Part Two

2011-10-25

"Our investigation and research of Duqu malware continues. In our previous report, we made two points:

1) there are more drivers than it was previously thought;

2) it is possible that there are additional modules.

Besides those key points, we concluded that unlike the massive Stuxnet infections, Duqu attacks are limited to an extremely small number of targets."

http://www.securelist.com/en/blog/208193197/The_Mystery_of_Duqu_Part_Two

Exclusive: Medtronic probes insulin pump risks

2011-10-25

"Security software maker McAfee, which has a health industry business, exposed the new vulnerability in one model of the Medtronic Paradigm insulin pump on Friday and believes there could be similar risks in others."

http://ca reuters.com/article/domesticNews/idCATRE79O8EP20111025

Huge threats still targeting power grids

2011-10-18

"Utilities have – as many predicted – realized that their grids are no longer isolated or protected from attackers."

http://www net-security.org/malware_news.php?id=1877

Inside a government computer attack exercise

2011-10-17

"To demonstrate the vulnerability, the Department of Homeland Security and Idaho National Laboratory in Idaho Falls recently showed reporters a cyberattack on a mock-up of a chemical facility."

http://www.cnn.com/2011/10/17/tech/innovation/cyberattack-exercise-idaho/index.html

DHS: Anonymous Interested in Hacking Nation's Infrastructure

2011-10-17

"The hacker collective known as Anonymous has expressed interest in hacking industrial systems that control critical infrastructures, such as gas and oil pipelines, chemical plants and water and sewage treatment facilities, according to a Department of Homeland Security bulletin."

http://www.wired.com/threatlevel/2011/10/hacking-industrial-systems/

Security upgrades required to counter worldwide cyberwar threats

2011-10-11

"Critical infrastructure such as industrial systems, transportation and power grids are easy targets for cyberattacks and people responsible for IT and national security are worried about the future, said Eugene Kaspersky, founder of Kaspersky Labs."

http://www.computerworlduk.com/news/security/3309685/security-upgrades-required-to-counter-worldwide-cyberwar-threats/

Zero-day flaws found in SCADA systems

2011-10-10

"An Italian security researcher recently disclosed details about several zero-day vulnerabilities in supervisory control and data acquisition (SCADA) systems from several vendors."

http://www.computerworld.com/s/article/359141

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. With the exception of this two-month issue, each issue includes information collected in the previous 28 to 31 days.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.

The public can view this document on the ICS-CERT web page at: http://www.us-cert.gov/control_systems/ics-cert/.

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

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:

- Billy Rios and Terry McCorkle, ICSA-11-279-03 - Unitronics UniOPC Server Input Handling Vulnerability Oct 6
- Billy Rios and Terry McCorkle, ICSA-11-285-01 - Honeywell TEMA Remote Installer ActiveX Oct 11
- Billy Rios and Terry McCorkle, ICSA-11-279-03A - Unitronics UniOPC Server Input Handling Vulnerability Oct 12
- Dillion Beresford, ICSA-11-294-01 - Progea Movicon Power HMI Vulnerabilities Oct 20
- Kuang-Chun Hung (Morgan) (ICST), ICSA-11-277-01 - Schneider Electric UnitelWay Buffer Overflow Oct 20

Researchers Currently Working with ICS-CERT

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

Ruben Santamarta
Kuang Chun Hung (ICST)
Jeremy Brown
Billy Rios
Eireann Leverett
Joel Langill
Yun Ting Lo (ICST)
Dillon Beresford
Terry McCorkle
Carlos Mario Penagos Hollmann
Michael Orlando
Knud Erik Hojgaard (nSense)
Secunia