Homeland Security

Daily Open Source Infrastructure Report 17 October 2013

Top Stories

- A former Halliburton Energy Services manager pleaded guilty to destroying evidence related to the 2010 Deepwater Horizon oil spill in the Gulf of Mexico. – *Associated Press* (See item **1**)
- Researchers found that the Automatic Identification System (AIS) tracking system on commercial and passenger ships is vulnerable to cyberattacks that could misdirect ships and spoof various signals. – *Softpedia* (See item **10**)
- Sixty-four Cleveland police officers were found guilty for various charges and will be disciplined in connection with their role in a 2012 police chase that resulted in 137 shots being fired at two unarmed occupants of a speeding car. – *CNN* (See item **24**)
- Oracle released its October Critical Patch Update (CPU) which includes patches for 127 security vulnerabilities across a range of products. – *The Register* (See item **25**)

Fast Jump Menu

PRODUCTION INDUSTRIES

SUSTENANCE and HEALTH

SERVICE INDUSTRIES

FEDERAL and STATE

Energy Sector

1. *October 16, Associated Press* – (International) **Ex-Halliburton manager pleads guilty.** A former Halliburton Energy Services manager pleaded guilty October 15 to destroying evidence in a 2010 oil spill in the Gulf of Mexico. The former employee of Halliburton, BP plc.'s contractor on the Deepwater Horizon drilling rig, instructed employees to delete data during a post-spill review of the cement job on BP's blown-out Macondo well.
   Source: http://www.lasvegassun.com/news/2013/oct/16/us-gulf-oil-spill-halliburton/

2. *October 16, Associated Press* – (Arizona; New Mexico; Colorado) **Contaminated gas went to 20 stores in NM, Arizona.** Western Refining is paying for repairs after a total of 20 stores in New Mexico and Arizona and 2 stores in Colorado received contaminated gasoline from the refinery. The company stated a gasket failed, allowing water to leak into a petroleum storage tank near Gallup.
   Source: http://www.myfoxphoenix.com/story/23667292/contaminated-gasoline-went-to-stores-in-az-co-nm

3. *October 14, KTLA 5 Los Angeles* – (California) **Buckled oil rig removed after threat to homes in Huntington Beach.** Crews removed a 60 foot oil derrick in Huntington Beach after it buckled October 14 and tilted over homes, prompting a 6 hour evacuation of the surrounding area. Authorities are investigating the cause of the derrick's failure.
   Source: http://ktla.com/2013/10/14/oil-rig-buckles-near-homes-above-power-lines-in-huntington-beach/

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

4. *October 16, Quincy Patriot Ledger* – (Massachusetts) **Pilgrim nuclear plant offline for 4th time this year.** The Pilgrim nuclear power plant in Plymouth automatically shut down October 14 due to a loss of offsite power caused by a power line failed during maintenance by utility company workers. The outage was the fourth thus far in 2013.
   Source: http://www.patriotledger.com/topstories/x1281960517/Pilgrim-nuclear-plant-offline-for-4th-time-this-year

5. *October 15, Denver Post* – (Colorado) **Radioactive gauge reported stolen out of truck in Thornton.** Colorado's Hazardous Materials and Waste Division asked for the public's help in locating a moisture density gauge containing radioactive materials that

was stolen from a parked truck October 13.
Source: http://www.denverpost.com/breakingnews/ci_24317673/radioactive-gauge-reported-stolen-out-truck-thornton

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

6. *October 15, SC Magazine* – (International) **New malware enables attackers to take money directly from ATMs.** Researchers at Safensoft and Trustwave identified and analyzed a piece of malware known as Ploutus that has been infecting ATMs in Mexico and allowing criminals to instruct the machines to dispense cash. The ATMs are infected after their CD-ROM drives are forced open, and instructions are given to compromised machines either by keypad sequences or by the interactive interface.
Source: http://www.scmagazine.com/new-malware-enables-attackers-to-take-money-directly-from-atms/article/316409/

7. *October 15, Ars Technica* – (International) **"Dexter" malware infects South African restaurants, costs banks millions.** Banks in South Africa sustained millions of dollars in losses after a new variant of the Dexter point-of-sale device malware was found to have compromised the accounts of potentially hundreds of thousands of customers.
Source: http://arstechnica.com/security/2013/10/dexter-malware-infects-south-african-restaurants-costs-banks-millions/

8. *October 15, KTVI 2 St. Louis* – (Illinois) **O'Fallon bank robbery suspect may be serial robber.** Police arrested a man in Swansea identified as a suspect in the October 15 robbery of a Bank of O'Fallon branch in Lincoln, and investigators believe he may be the same man responsible for at least six other bank robberies.
Source: http://fox2now.com/2013/10/15/police-searching-for-bank-robbers-near-belleville/

9. *October 15, Greater Alexandria Patch* – (Virginia) **Police arrest suspect in 'Beacon Hill Bandit' bank robberies.** Police arrested a man in Alexandria believed to be the "Beacon Hill Bandit" responsible for robbing the same TD Bank branch six times

between 2010 and 2013.
Source: http://greateralexandria.patch.com/groups/around-town/p/police-arrest-suspect-in-beacon-hill-bandit-bank-robberies

[Return to top]

Transportation Systems Sector

10. *October 16, Softpedia* – (International) **Global vessel tracking systems vulnerable to hacker attacks, experts warn.** Researchers from Trend Micro found that the Automatic Identification System (AIS), a tracking system that relies on GPS installed on some commercial and all passenger ships, are vulnerable to cyberattacks where hackers can hijack the communications of ships, disable the AIS, create fake ship signals, and trigger fake SOS or collision alerts.
Source: http://news.softpedia.com/news/Global-Vessel-Tracking-Systems-Vulnerable-to-Hacker-Attacks-Experts-Warn-391628.shtml

11. *October 16, West Hartford News* – (Connecticut) **Fatal crash in West Hartford closes I-84.** A fatal multiple-car crash on Interstate 84 in West Hartford killed one and closed all lanes of Interstate 84 eastbound and two entrance ramps October 14.
Source:
http://www.westhartfordnews.com/articles/2013/10/16/news/doc525c6490a438c057229630.txt

12. *October 16, Associated Press* – (California) **Employee arrested in LA airport dry ice bombs.** An airport employee was arrested October 15 in connection with dry ice explosions at Los Angeles International Airport after one exploded device was found in an employee restroom October 13 and remnants of another exploded device were found on the tarmac outside the international terminal October 14.
Source: http://news.msn.com/crime-justice/employee-arrested-in-la-airport-dry-ice-bombs

13. *October 15, KFSN 30 Fresno* – (California) **Northbound Highway 99 in Goshen open after deadly crash.** One person was killed and two other were injured in a three-vehicle accident involving two semi-trucks and a car on northbound Highway 99 in Fresno. Northbound lanes were closed as well as the northbound onramp from Highway 198 to Highway 99 for an undisclosed amount of time October 15.
Source: http://abclocal.go.com/kfsn/story?section=news/local&id=9287450

14. *October 13, KABC 7 Los Angeles* – (California) **Dana Point car crash: 2 dead, 3 injured in violent accident.** Two people died and three people were injured in a four-vehicle accident on Coast Highway and Beach Road in Dana Point, closing a portion of the road in both directions for an undisclosed amount of time October 13.
Source:
http://abclocal.go.com/kabc/story?section=news/local/orange_county&id=9285732

For another story, see item **23**

[Return to top]

Food and Agriculture Sector

15. *October 15, U.S. Food and Drug Administration* – (Michigan) **Best Value, Inc., recalls PRAN brand turmeric powder due to elevated levels of lead.** Best Value, Inc. of Detroit voluntarily recalled PRAN Turmeric Powder because it was found to contain high levels of lead. The U.S. Food and Drug Administration initiated the recall after discovery of the problem through product sampling.
    Source: http://www.fda.gov/Safety/Recalls/ucm371042.htm

16. *October 14, U.S. Food and Drug Administration* – (National) **Yoder's Country Market, Inc. issues allergy alert on gift boxes containing 11 oz. bags of honey roasted peanuts distributed in December 2012.** Yoder's Country Market, Inc. recalled 11 ounce bags of Honey Roasted Peanuts contained in gift boxes distributed in December 2012 because they may contain undeclared milk and wheat. The recall was initiated after the distributor, Dutch Valley Food Development of Myerstown, Pennsylvania, notified Yoder's Country Market, Inc. of their recall in September 2013.
    Source: http://www.fda.gov/Safety/Recalls/ucm371002.htm

[Return to top]

Water and Wastewater Systems Sector

17. *October 15, WCNC 6 Charlotte*– (South Carolina) **Boil water advisory in place after Tega Cay water main break.** Officials announced a 48-hour boil water advisory in Tega Cay after a major water main break October 15 caused when a 12-inch water line broke. Residents were advised that they could shower and bathe with the water.
    Source: http://www.wcnc.com/news/local/Water-main-break-behind-flooded--227892651.html

[Return to top]

Healthcare and Public Health Sector

18. *October 16, Associated Press* – (Ohio) **Hospital patient found with 3 guns after threats.** Police are investigating after a patient from Bethesda North Hospital in Montgomery, Ohio, threatened staff October 10. Authorities seized a duffel bag full of guns and other weapons from the patient after workers alerted police.
    Source: http://www.dispatch.com/content/stories/local/2013/10/16/hospital-patient-found-with-3-guns-after-threats.html

19. *October 15, Associated Press* – (National) **FDA alerts doctors to recalled B Braun antibiotic due to floating particles in drug vials.** The U.S. Food and Drug Administration alerted doctors October 15 that B. Braun Medical recalled Cefepime for Injection USP and Dextrose Injection USP injectable antibiotics due to floating particles found in vials of the drug.

Source: http://www.washingtonpost.com/business/fda-alerts-doctors-to-recalled-b-braun-antibiotic-due-to-floating-particles-in-drug-vials/2013/10/15/1ff87b24-35e7-11e3-89db-8002ba99b894_story.html

20. *October 15, WDJT 58 Milwaukee* – (Wisconsin) **Electrical fire and evacuation at Zablocki V.A. Center.** Zablocki Veterans Affairs Medical Center in Milwaukee was evacuated October 15, displacing 117 residents due to an electrical short in the building. The displaced veterans were placed in other facilities until repairs are made.
Source: http://www.cbs58.com/news/local-news/Electrical-fire-and-evacaution-at-Zablocki-VA-Center-227885991.html

[Return to top]

Government Facilities Sector

21. *October 16, KMGH 7 Denver* – (Colorado) **Denver's West High School reopens after bed bugs exterminated from classroom.** Officials reopened West High School in Denver October 16 after closing the school October 11 in order to remove bed bugs that were found in a classroom.
Source: http://www.thedenverchannel.com/news/local-news/denvers-west-high-school-reopens-after-bed-bugs-exterminated-from-classroom

22. *October 16, Saginaw News* – (Michigan) **Vandalism cancels classes at Bridgeport High School.** School officials cancelled classes at Bridgeport High School in Bridgeport Township October 16 in order to assess the damage after they found several windows broken at the building.
Source:
http://www.mlive.com/news/saginaw/index.ssf/2013/10/vandalism_cancels_classes_at_b.html

23. *October 15, Cedar Rapids Gazette* – (Iowa) **Audit shows another $195,000 linked to alleged Iowa DOT land sales scheme.** Three men, including a former Iowa Department of Transportation (DOT) employee, were charged in connection with a money-laundering and kickback scheme to steal more than $775,000 from the Iowa DOT. Authorities are still investigating and gathering information.
Source: http://amestrib.com/sections/news/ames-and-story-county/audit-shows-another-195000-linked-alleged-iowa-dot-land-sales

For another story, see item **32**

[Return to top]

Emergency Services Sector

24. *October 16, CNN* – (Ohio) **Police chief: 64 Cleveland officers broke rules in shooting.** Sixty-four Cleveland police officers were found guilty for various charges

and will be disciplined in connection with their role in a 2012 police chase that resulted in 137 shots being fired at two occupants of a speeding car. The two individuals in the car were killed and an investigation determined they were unarmed.
Source: http://www.cnn.com/2013/10/16/justice/cleveland-police-shooting/index.html

[Return to top]

Information Technology Sector

25. *October 16, The Register* – (International) **Oracle drops shedload of CRITICAL vuln-busting Java patches.** Oracle released its October Critical Patch Update (CPU) which includes patches for 127 security vulnerabilities across a range of products. Fifty-one vulnerabilities were addressed in Java, including 12 that could allow attackers to take full control of targeted machines without authentication.
Source: http://www.theregister.co.uk/2013/10/16/oracle_quarterly_patch_batch/

26. *October 16, Softpedia* – (International) **5 vulnerabilities fixed with release of Chrome 30.0.1599.101.** Google released the latest update for its Chrome browser, closing five security issues.
Source: http://news.softpedia.com/news/5-Vulnerabilities-Fixed-with-Release-of-Chrome-30-0-1599-101-391599.shtml

27. *October 16, Softpedia* – (International) **Researchers identify two sandbox escape vulnerabilities in IBM SDK for Java 7.0.** Researchers from Security Explorations identified and reported two Java sandbox escape vulnerabilities affecting Java SDK for Java Technology Edition, version 7.0 SR5. The researchers sent a report and proof-of-concept to IBM October 16.
Source: http://news.softpedia.com/news/Researchers-Identify-Two-Sandbox-Escape-Vulnerabilities-in-IBM-SDK-for-Java-7-0-391740.shtml

28. *October 16, CNET* – (International) **Microsoft-DS no longer hackers' top target.** Akamai stated in their "State of the Internet" report that Microsoft-DS, also known as Port 445, was no longer the primary path of attack for attackers, for the first time since Akamai began gathering data on attack vectors in 2008. Cybercriminals have instead changed to targeting users through HTTP Port 80 and SSL Port 443.
Source: http://news.cnet.com/8301-1009_3-57607722-83/microsoft-ds-no-longer-hackers-top-target/

29. *October 16, Softpedia* – (International) **Rapid7.com hijacking: Theft of employee credentials, not faxed DNS change request.** Rapid7 reported that a recent attack by hacktivist group KDMS Team did not use a fax request to Register.com to change Rapid7 and Metasploit's DNS records, as previously reported. Instead, Rapid7 found that the attackers used social engineering to obtain employee credentials for use in the DNS record change.
Source: http://news.softpedia.com/news/Rapid7-com-Hijacking-Theft-of-Employee-Credentials-Not-Faxed-DNS-Change-Request-391641.shtml

30. *October 15, Softpedia* – (International) **Info stealer trojan Nemim used against organizations from the U.S. and Japan.** Symantec researchers found that the Nemim trojan is being used in a campaign targeting U.S. and Japanese organizations to collect information from infected computers, and that the campaign and trojan appear similar to the Egobot trojan that has been used to target South Korean organizations since 2009.
Source: http://news.softpedia.com/news/Info-Stealer-Trojan-Nemim-Used-Against-Organizations-from-the-US-and-Japan-391292.shtml

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

31. *October 15, WTVT 13 Tampa Bay* – (Florida) **HAZMAT team investigates ‘unknown substance’ at mall.** Investigators are looking into an October 15 incident at a store inside the Westfield Southgate mall in Sarasota where someone threw a crushed substance into the store before fleeing the area. The mall was locked down for several hours until officials could determine if the substance posed any danger.
Source: http://www.myfoxtampabay.com/story/23695903/2013/10/15/hazmat-team-investigates-unknown-substance-at-mall

32. *October 14, KSLA 12 Shreveport* – (Louisiana) **Walmart shelves in Springhill, Mansfield, cleared in EBT glitch.** Springhill and Mansfield police departments were called into two Walmart stores for crowd control while shoppers using EBT cards stocked up on food while the system suffered a glitch that showed no spending limits on the cards. Xerox, the vendor for the EBT system, suffered a power outage and after the power was restored the system was not completely functional in some areas.
Source: http://www.ksla.com/story/23679489/walmart-shelves-in-springhill-mansfield-cleared-in-ebt-glitch

[Return to top]

Dams Sector

Nothing to report

[Return to top]

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.