Daily Open Source Infrastructure Report
16 December 2014

Top Stories

- Heavy rains starting December 12 flooded several roadways in southern California and caused a mudslide that closed a stretch of the Pacific Coast Highway in Ventura County, while rail service in the area was suspended. – *KNBC 4 Los Angeles* (See item **10**)
- A gas leak from an ice-resurfacing machine at the Poppy Waterman Ice Arena in Lake Delton, Wisconsin, sent 81 people to area hospitals for carbon monoxide poisoning after experiencing nausea, dizziness, and headaches December 13. – *Milwaukee Journal Sentinel; Associated Press* (See item **26**)
- Between 3,000 and 5,000 staff and visitors were evacuated from the American Museum of Natural History in New York City December 12 after a fire sparked by maintenance work on an air conditioning unit outside of the building sent smoke into the museum. – *WCBS 2 New York City* (See item **30**)
- Several thousand U.S. retailers using older models of Equinox Payments' Hypercom credit card payment terminals experienced an outage December 7 when a security mechanism was triggered by the expiration of the products' cryptographic certificate that was created in 2004 with a 10-year expiry date. – *Krebs on Security* (See item **33**)

Fast Jump Menu

Energy Sector

1. *December 14, Associated Press* – (Vermont) **13,000 still without power in Vermont after storm.** More than 13,000 Vermont Electric Cooperative customers in Vermont remained without power December 13 following a powerful storm and heavy snow that cut out power to about 100,000 customers December 11.
   Source: http://www.rep-am.com/articles/2014/12/15/news/national/849429.txt

2. *December 13, Peninsula Daily News* – (Washington) **Copper thief cuts power to 2,000 after damaging Clallam Public Utility District substation west of Port Angeles.** Copper thieves damaged three voltage regulators and knocked out power to about 2,000 residents in the Elwha Valley for nearly 12 hours December 13. Estimated damages totaled $120,000.
   Source:
   http://www.peninsuladailynews.com/article/20141214/news/312149959/copper-thief-cuts-power-to-2000-after-damaging-clallam-public

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *December 13, Bloomberg News* – (Pennsylvania) **Pennsylvania nuclear reactor shut down after water leak.** The operators of the Susquehanna nuclear power plant near Berwick shut down one of the plant's reactors December 13 due to a small water leak within the unit's containment structure. The plant's other reactor continued to operate and operators were planning repairs to close the leak.
   Source: http://www.bloomberg.com/news/2014-12-13/pennsylvania-nuclear-reactor-shut-down-after-water-leak.html

[Return to top]

Critical Manufacturing Sector

4. *December 12, Detroit News* – (National) **Mazda recalls 330,000 vehicles for driver-side air bags.** Mazda Motor Co. announced December 12 that it was expanding its recall for vehicles equipped with airbag inflators manufactured by Takata to include 330,000-model year 2004-2008 Mazda6 and RX-8 vehicles nationwide. The airbag inflators can send metal fragments into the passenger cabin upon inflation, posing a threat to occupants.
   Source: http://www.detroitnews.com/story/business/autos/foreign/2014/12/12/mazda-recalls-vehicles-driver-side-air-bags/20294363/

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

5. *December 13, Associated Press* – (Pennsylvania) **Bail bondsman charged with writing fraudulent bonds.** A Berks County bail bondsman and three other employees of Ace Bail Bonds were charged December 12 for allegedly writing $2 million in fraudulent bail bonds between August and September.
   Source: http://www.nbcphiladelphia.com/news/local/Bail-Bondsman-Charged-With-Writing-Fraudulent-Bonds-285656571.html

6. *December 12, Chicago Tribune* – (Illinois) **'Play-Along Bandit' sought by the FBI.** The FBI asked for the public's help in finding a suspect known as the "Play-Along Bandit" suspected in at least five Chicago bank robberies since October 18. The most recent robbery tied to the suspect took place at a Harris Bank branch December 7.
   Source: http://www.chicagotribune.com/news/local/breaking/chi-playalong-bandit-sought-by-the-fbi-20141212-story.html

7. *December 12, U.S. Securities and Exchange Commission* – (New York) **Court orders former managing director of the NASDAQ Stock Market to disgorge more than $898,000 in insider trading profits.** A former managing director of the NASDAQ Stock Market was ordered to disgorge $898,107.92 in illicit profits plus interest for engaging in insider trading using nonpublic information entrusted to him by NASDAQ and listed companies ahead of nine announcements between August 2006 and July 2009.
   Source: http://www.sec.gov/litigation/litreleases/2014/lr23156.htm

8. *December 12, U.S. Securities and Exchange Commission* – (New York) **SEC charges Manhattan-based attorney with conducting Ponzi scheme.** The U.S. Securities and Exchange Commission filed charges December 12 against a New York City-based attorney for allegedly conducting a $5 million Ponzi scheme that purported to invest clients' investments in an investment fund that the attorney was not in fact affiliated with. Parallel criminal charges were also filed by the U.S. Attorney's Office for the Southern District of New York.
   Source: http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543693087

[Return to top]

Transportation Systems Sector

9. *December 13, Washington Post* – (Maryland) **Southwest Airlines plane lands safely**

at BWI after being struck by bird. A Southwest Airlines flight en route to Detroit from San Antonio was forced to make an emergency landing at Baltimore-Washington International Marshall Airport December 12 after being struck by a bird. The plane landed safely with 142 passengers and 5 crewmembers on board and was taken out of service to be inspected without continuing on to its final destination.
Source: http://www.washingtonpost.com/local/southwest-airlines-plane-lands-safely-at-bwi-after-being-struck-by-bird/2014/12/13/a661eb5a-8280-11e4-81fd-8c4814dfa9d7_story.html

10. *December 12, KNBC 4 Los Angeles* – (California) **SoCal roadways closed by mud and floods, snarling commute.** Several freeways were closed in southern California December 12 after heavy rains flooded northbound lanes of 170 Freeway in North Hollywood and a stretch of the Pacific Coast Highway in Ventura County due to a mudslide. The severe weather conditions also led to a suspension of the Amtrak Pacific Surfliner service and a downed tree caused delays for the Gold Line railway in Pasadena.
Source: http://www.nbclosangeles.com/news/local/Mud-and-Floods-Close-SoCal-Freeways-in-Morning-Storm-285608191.html

11. *December 12, WGAL 8 Lancaster* – (Pennsylvania) **80+ gallons of diesel fuel spilled in accident on Manheim Pike.** HAZMAT crews worked to cleanup more than 80 gallons of diesel fuel that spilled onto Manheim Pike/Route 72 in Lancaster December 12, closing the road for 5 hours.
Source: http://www.wgal.com/news/southbound-lanes-of-manheim-pike-temporarily-closed-in-lancaster/30198464

12. *December 11, Athens Daily Review* – (Texas) **Copper wire stolen.** Two individuals were arrested December 10 for allegedly stealing up to $20,000 worth of copper wire from a Union Pacific Railroad control station near Athens, Texas, causing up to $100,000 in damage to transportation communications equipment or devices at the facility.
Source: http://www.athensreview.com/news/local_news/copper-wire-stolen/article_8e3d5f12-8188-11e4-aabc-27921d33991d.html

For another story, see item **17**

[Return to top]

Food and Agriculture Sector

13. *December 15, Associated Press* – (South Dakota) **Grain bin collapses at Britton elevator.** Authorities are investigating after a 40,000-bushel grain bin at the Wheaton Dumont Co-Op elevator in Britton, South Dakota, collapsed December 14. The collapse damaged about 20,000 bushels of grain and destroyed conveyors and other overhead equipment.
Source: http://www.argusleader.com/story/news/crime/2014/12/15/grain-bin-collapses-britton-elevator/20428503/

14. *December 12, Janesville Gazette* – (Wisconsin) **Grain bin near Evansville is total loss from Friday fire, chief says.** A grain bin holding about 1,400 bushels of corn at Arnold Farms near Evansville was rendered a total loss following a December 12 fire. The cause of the fire is under investigation.
Source:http://www.gazettextra.com/20141212/grain_bin_near_evansville_is_total_loss_from_friday_fire_chief_says

[Return to top]

Water and Wastewater Systems Sector

15. *December 12, KGTV 10 San Diego* – (California) **Man rescued after falling into La Jolla water tank.** A worker was rescued and transported to an area hospital after falling approximately 20-feet into an empty underground water tank in La Jolla December 12. The San Diego Fire-Rescue Department reported that the man and another individual were climbing out of the tank after coating its interior with an epoxy before the fall which raised concerns about the possibility of exposure to fumes in a confined space.
Source: http://www.10news.com/news/man-falls-into-la-jolla-water-tank

[Return to top]

Healthcare and Public Health Sector

Nothing to report

[Return to top]

Government Facilities Sector

16. *December 13, Washington Post* – (Maryland) **Former Pr. George's housing official indicted on wire fraud, conspiracy charges.** A former Prince George's County Housing Authority official and her husband was indicted the week of December 8 on charges related to an alleged scheme that funneled money from the U.S. Department of Housing and Urban Development's Section 8 Housing Choice Voucher Program to a personal bank account between 2007 and 2012 obtaining a total of $109,823 in subsidy payments. The couple is facing 15 criminal counts including conspiracy to commit wire fraud, wire fraud, and money laundering.
Source: http://www.washingtonpost.com/local/md-politics/former-pr-georges-housing-official-indicted-on-wire-fraud-conspiracy-charges/2014/12/13/4a07b67a-823d-11e4-81fd-8c4814dfa9d7_story.html

17. *December 13, Reuters* – (National) **New York man pleads guilty to fake anthrax, ricin attacks.** A Cicero, New York man pleaded guilty to 2 federal counts of conveying false information and hoaxes December 13 for mailing 20 death-threat letters laced with harmless white powder claimed to be either anthrax or ricin to

schools, U.S. officials and lawmakers between 1997 and 2012.
Source: http://www.reuters.com/article/2014/12/13/us-usa-new-york-crime-idUSKBN0JR04720141213

18. *December 11, WEWS 5 Cleveland* – (Ohio) **St. Rita Elementary School and University School Shaker Campus closed due to flu outbreak.** St. Rita Elementary School in Solon and University School's Shaker Heights campus were both closed December 10 due to a flu outbreak after students experienced symptoms of fever, nausea, and coughing. Classes at St. Rita Elementary School were scheduled to resume December 15.
Source: http://www.newsnet5.com/news/local-news/oh-cuyahoga/st-rita-elementary-school-closed-due-to-illness

[Return to top]

Emergency Services Sector

19. *December 15, WTTG 5 Washington, D.C.* – (Maryland) **Suspect crashes stolen ambulance in Greenbelt.** One person was killed and two other were injured, including the alleged carjacker, December 14 when a stolen Branchville Volunteer Fire Department ambulance crashed into 11 cars before overturning in a Greenbelt, Maryland restaurant parking lot. Authorities are investigating the accident.
Source: http://www.myfoxdc.com/story/27625719/suspect-crashes-stolen-ambulance-in-greenbelt

For another story, see item **24**

[Return to top]

Information Technology Sector

20. *December 15, Softpedia* – (International) **CloudFlare SSL certificate used for phishing scam.** A researcher with Malwarebytes identified a new phishing email campaign that utilized a free CloudFlare certificate in order to make a malicious link appear more trustworthy. CloudFlare has since revoked the certificate.
Source: http://news.softpedia.com/news/CloudFlare-SSL-Certificate-Used-For-Phishing-Scam-467356.shtml

21. *December 15, Softpedia* – (International) **SoakSoak malware campaign affects over 100,000 websites.** A Sucuri researcher reported that malware delivered from the Russian Web site soaksoak.ru has affected over 100,000 WordPress Web sites adding a code that adds a malicious JavaScript on every page viewed on the affected sites. Google then blacklisted more than 11,000 domains connected to the malware.
Source: http://news.softpedia.com/news/SoakSoak-Malware-Campaign-Affects-Over-100-000-Websites-467506.shtml

22. *December 12, Securityweek* – (International) **Ursnif malware steals data, infects files**

in US, UK. Trend Micro researchers detected an increase in the number of Ursnif malware infections caused by a variant known as PE_URSNIF.A-O that is capable of infecting files as well as stealing passwords and other information. The largest number of the new infections were found in the U.S. and U.K.
Source: http://www.securityweek.com/ursnif-malware-steals-data-infects-files-us-uk

23. *December 12, The Register* – (International) **Batten down the patches: New vuln found in Docker container tech.** A security researcher identified an arbitrary code execution vulnerability in Docker that was introduced in a November patch and could be exploited by including malicious .xz binaries in image files. The developers of Docker released a new patch that closes the vulnerability, and all users were advised to apply the patch as soon as possible.
Source: http://www.theregister.co.uk/2014/12/12/docker_vulnerability/

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: http://www.it-isac.org

[Return to top]

Communications Sector

24. *December 13, WNYT 13 Albany* – (New York) **911 services restored in Canajoharie.** All phone services, including 9-1-1 service, were restored December 13 to Frontier Communications customers in Canajoharie after a small fire from a gas leak damaged a line and knocked out service December 12.
Source: http://wnyt.com/article/stories/s3648721.shtml

[Return to top]

Commercial Facilities Sector

25. *December 15, Securityweek* – (International) **Honeywell OPOS suite affected by serious vulnerability.** Researchers with the Computer Emergency Response Team Coordination Center at Carnegie Mellon University (CERT/CC) identified a stack buffer overflow vulnerability that affects the HWOPOSScale.ocx and HWOPOSSCANNER.ocx components of Honeywell's OLE for Retail Point-of-Sale (OPOS) Suite versions prior to 1.13.4.15 which can be exploited for remote code execution on vulnerable systems. Honeywell has released a patch to address the issue.
Source: http://www.securityweek.com/honeywell-opos-suite-affected-serious-vulnerability

26. *December 14, Milwaukee Journal Sentinel; Associated Press* – (Wisconsin) **Dozens sickened by carbon monoxide at Lake Delton ice rink.** At least 81 individuals at the

Poppy Waterman Ice Arena in Lake Delton were treated for symptoms related to carbon monoxide exposure December 13 due to a leak that was discovered coming from one of the rink's propane-fueled resurfacing machines. Authorities are investigating the incident and an inspection of the equipment was scheduled.
Source: http://www.jsonline.com/news/wisconsin/dozens-reportedly-sickened-by-carbon-monoxide-at-lake-delton-ice-rink-b99408550z1-285749581.html

27. *December 13, KNTV 11 San Jose* – (California) **Residents at Redwood City mobile home parks ordered to evacuate due to safety risks, flooding.** Dozens of residents were displaced from about 50 mobile homes at the Le Mar Trailer Park and RC Mobile Home Park in Redwood City after officials ordered their evacuation December 11 due to possible health and safety risks caused by standing water. Heavy rains that moved through the area December 10 caused flooding that prompted officials to red-tag homes inside the mobile home parks.
Source: http://www.nbcbayarea.com/news/local/Redwood-City-Mobile-Home-Park-Flooded-Residents-Forced-to-Evacuate-285559061.html

28. *December 13, Chicago Tribune* – (Illinois) **9 charged in retail theft ring, including mother and daughter.** Nine individuals were arrested and charged December 12 for their alleged involvement in a theft ring that stole more than $21,000 worth of merchandise from at least five Chicago retail stores between November 19 and December 10. Authorities are investigating to determine if the suspects are connected to similar retail thefts in Chicago.
Source: http://www.chicagotribune.com/news/local/breaking/chi-9-accused-of-retail-theft-ring-20141213-story.html

29. *December 13, KABC 7 Los Angeles* – (California) **Military ordnance prompts evacuations in Torrance.** The Turner's Outdoorsman store in Torrance and nearby businesses were evacuated for almost 2 hours December 13 after a suspicious military ordnance was brought inside the sporting goods store. The Los Angeles County sheriff's bomb squad collected the device and secured the scene before deeming the area clear.
Source: http://abc7.com/news/military-ordnance-prompts-evacuations-in-torrance-/435913/

30. *December 12, WCBS 2 New York City* – (New York) **Small fire prompts evacuation of American Museum of Natural History.** Between 3,000 and 5,000 staff and visitors were evacuated from the American Museum of Natural History in New York City December 12 while firefighters ventilated the building following a small fire that was sparked during maintenance work on an air conditioning unit mounted outside of the museum. The museum suffered minor water damage from the building's sprinkler system and was expected to reopen December 13.
Source: http://newyork.cbslocal.com/2014/12/12/small-fire-prompts-evacuation-of-american-museum-of-natural-history/

31. *December 12, Reuters* – (Maryland; Virginia) **Maryland man admits to six 'bottle**

bomb' stunts at movie theaters. A Maryland man pleaded guilty December 12 to charges that he detonated six "bottle bombs" at six separate movie theaters across Maryland and Virginia between April and May in an attempt to induce panic.
Source: http://www.reuters.com/article/2014/12/12/us-usa-bottlebombs-maryland-idUSKBN0JQ2B020141212

32. *December 12, WUSA 9 Washington, D.C.* – (Washington, D.C.) **Mouse plagued Harris Teeter closes again, 'voluntarily'.** A Washington, D.C. Harris Teeter grocery store reclosed indefinitely December 10 due to an "imminent health hazard" that required the execution of pest control and sanitation procedures. The store was cited for 13 violations including a rodent infestation and was ordered closed by District of Columbia health officials December 8 before it briefly reopened December 10 after passing a second inspection.
Source: http://www.wusa9.com/story/news/investigations/russ-ptacek/2014/12/10/harris-teeter-health-suspension/20214527/

33. *December 12, Krebs on Security* – (National) **'Security by antiquity' bricks payment terminals.** Equinox Payments officials reported that U.S. retailers using certain models of its Hypercom credit card payment terminals experienced an outage December 7 when a security mechanism was triggered by the expiration of the products' cryptographic certificates that were assigned a 10 year expiry date in 2004. Company officials are working to replace the certificates and return thousands of the bricked terminals to an operational state.
Source: http://krebsonsecurity.com/2014/12/security-by-antiquity-bricks-payment-terminals/

[Return to top]

Dams Sector

34. *December 11, Associated Press* – (Texas) **LCRA breaks ground, new reservoir in South Texas.** The Lower Colorado River Authority (LCRA) commenced work on a reservoir off the main channel of the lower Colorado River in southern Texas, which will increase water supplies to cities, homes, and businesses in central Texas December 10. The Texas Water Development Board granted LCRA $250 million for the construction of the reservoir that is expected to be complete in 2017.
Source: http://kxan.com/ap/lcra-breaks-ground-new-reservoir-in-south-texas-2/

[Return to top]

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