



Daily Open Source Infrastructure Report 15 May 2015

Top Stories

- An estimated 198,000 gallons of household wastewater spilled into La Volla Creek in Corpus Christi, Texas, May 13 from a flooded sewage line. – *Corpus Christi Caller-Times* (See item [18](#))
- The U.S. Attorney’s Office in Tampa announced May 13 that CVS Health Corp., will pay \$22 million in a settlement to resolve allegations that 2 of its pharmacies in Florida sold non-prescribed painkillers. – *Reuters* (See item [19](#))
- OSISoft advised customers to mitigate an incorrect default permissions vulnerability in its PI Asset Framework (PI AF) that could potentially lead to information disclosure, data tampering, privilege escalation, and/or denial-of-service (DoS) conditions. – *Securityweek* (See item [26](#))
- Downingtown, Pennsylvania police declared the North Park Plaza strip mall a total loss May 14 after 10 businesses and both floors of the mall were severely damaged in a May 12 fire. – *Chester County Daily Local News* (See item [28](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. *May 13, Dark Reading* – (International) **Oil & gas firms hit by cyberattacks that forgo malware.** Panda Lab researchers discovered a unique targeted attack campaign dubbed Phantom Menace that has infiltrated and stolen credentials from 10 international oil and gas maritime transportation companies since August 2013, via a spear-phishing email containing a fake Adobe PDF file utilizing a file transfer protocol (FTP) server. The attackers contact oil brokers and request a fee in exchange for fake barrels of oil sold at a discounted rate, which are never delivered.
Source: <http://www.darkreading.com/attacks-breaches/oil-and-gas-firms-hit-by-cyberattacks-that-forgo-malware/d/d-id/1320417>

For another story, see item [26](#)

[\[Return to top\]](#)

Chemical Industry Sector

2. *May 13, Wilkes-Barre Times Leader* – (Pennsylvania) **Crews responding to commercial structure fire at Acton Technologies near Pittston.** The Acton Technologies chemical plant in Jenkins Township was evacuated May 13 due to a commercial structure fire that left one person injured and caused an unknown amount of chemicals to enter a nearby creek, turning it white. Officials also evacuated and dismissed Pittston Area High School because of the fire.
Source: http://www.timesleader.com/news/home_top-news/153466962/

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

3. *May 14, WLKY 32 Louisville* – (Ohio) **Ohio nuclear plant resumes operations after steam leak.** FirstEnergy Corp., officials reported that the David-Besse nuclear power plant in Oak Harbor resumed operations May 12 and would be back at full power May 14, following the discovery of a steam leak that led to a manual shutdown of the plant May 9. Officials are investigating the cause of the leak and determining whether or not it was an isolated incident.
Source: <http://www.wlky.com/news/Ohio-nuclear-power-plant-resumes-operations-after-steam-leak/33015036>

For another story, see item [26](#)

[\[Return to top\]](#)

Critical Manufacturing Sector

4. *May 14, CNN* – (International) **Honda recalls 5 million cars as airbag woes spread.** Honda Motor Co., announced a recall May 14 for 4.89 million model year 2002 – 2008

vehicles spanning 14 models including Civic and CR-V series due to issues with airbags manufactured by Takata Corp., that could cause them to inflate prematurely or explode, increasing risks of crashes and injury. Over 3 million vehicles included in the recall are outside of Japan.

Source: <http://money.cnn.com/2015/05/14/autos/honda-airbag-recall/>

5. *May 13, Associated Press* – (Iowa) **2 Iowa wheel manufacturing plants cited for improperly handling, storing hazardous waste.** The U.S. Environmental Protection agency reported May 13 that GKN Armstrong Wheels had agreed to pay penalties of over \$150,000 after inspections of 2 plants in Estherville and Armstrong revealed that the company violated waste regulations by disposing hazardous waste without an appropriate permit, and failed to adhere to universal waste and used oil regulations.
Source: <http://www.greenfieldreporter.com/view/story/f84b1d2d1e1246b391a3a4140ea98d12/IA--EPA-Violations-Iowa>
6. *May 13, Car Connection* – (National) **2011-12 Chevrolet Malibu, 2015 Chevrolet Colorado & GMC Canyon recalled: 522,000 vehicles affected.** General Motors issued 2 recalls for 437,045 model year 2011 – 2012 Chevrolet Malibu vehicles in the U.S. for an issue with the seat belt cable connectors that could cause belts to break or separate from the vehicle, and for 49,309 model year 2015 Chevrolet Colorado trucks in the U.S. due to an issue with seat frames that could cause them to separate from the vehicle in a collision.
Source: http://www.thecarconnection.com/news/1098274_2011-12-chevrolet-malibu-2015-chevrolet-colorado-gmc-canyon-recalled-522000-vehicles-affected
7. *May 13, U.S. Department of Labor* – (Illinois) **Workers face risk of injury from machinery, chemical and fire hazards at Vandalia, Illinois, metal tube manufacturing plant.** The Occupational Safety and Health Administration cited All Steel Products, Inc., of Vandalia May 13 for 27 safety and health violations, including exposing workers to risks of lacerations, amputations, and potential explosions and fire by ignoring standard safety rules for machines and storing flammable materials in open containers near propane heaters. Proposed fines total \$109,000.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=27969
8. *May 13, Autoblog* – (National) **FCA expands Jeep Cherokee recall to 68k more vehicles.** Fiat Chrysler Automobiles (FCA) US LLC expanded an airbag software update May 12 to include 230,240 model year 2014 – 2015 Jeep Cherokee vehicles for an issue with the side-curtain and seat-mounted airbags that could cause them to inadvertently deploy in harsh, off-road environments.
Source: <http://www.autoblog.com/2015/05/13/jeep-cherokee-recall-expanded/>

For another story, see item [26](#)

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

9. *May 13, Reuters* – (Connecticut) **Connecticut fund executive faces new SEC fraud charges.** The U.S. Securities and Exchange Commission charged and froze the assets of a former Oak Investment Partners venture capital executive from Greenwich, May 13, alleging that the suspect transferred \$27.5 million worth of investors' funds to himself, induced his firm to overpay for investments into 2 Asian e-commerce companies for which he pocketed \$20 million, and induced the firm to pay I-Cubed Domains LLC \$7.5 million for its stake in an e-commerce company without disclosing that he and his wife owned I-Cubed Domains and had purchased the stake for \$2 million.
Source: <http://www.reuters.com/article/2015/05/13/sec-ahmed-fraud-idUSL1N0Y42NC20150513>
10. *May 13, Philadelphia Business Journal* – (Pennsylvania) **Delco mortgage lender charged with \$9.7M fraud scheme.** A former co-owner of Folsom-based Capital Financial Mortgage Corporation was charged May 13 for his role in a \$9.7 million mortgage fraud scheme in which he allegedly defrauded lenders including Wells Fargo & Co., and Customers Bank into purchasing second mortgages that he represented as first mortgages and defrauded other lenders that loaned money to the company on a warehouse line of credit. Authorities claim he used the fraudulent profits to pay for personal expenses.
Source: http://www.bizjournals.com/philadelphia/morning_roundup/2015/05/delco-mortgage-lender-charged-with-9-7m-fraud.html
11. *May 13, Lake View Patch* – (Illinois) **FBI increases reward for serial 'Bandage Bandit' bank robbery suspect.** The FBI increased the reward for information leading to the arrest of the bank robber dubbed the "Bandage Bandit" to \$10,000, after a May 9 robbery at a Chase Bank in Chicago was attributed to him, bringing the total to 5 robberies since March.
Source: <http://patch.com/illinois/lakeview/fbi-increases-reward-serial-bandage-bandit-bank-robber-suspect>

[\[Return to top\]](#)

Transportation Systems Sector

12. *May 14, St. Louis Post-Dispatch* – (Missouri) **I-55 reopened at Festus after cleanup of tanker's spilled chemical.** Interstate 55 in Festus reopened May 14 after closing

overnight May 13 while crews cleared a chemical spill from the roadway after a semi-truck carrying ammonium nitrate crashed on a ramp.

Source: http://www.stltoday.com/news/local/crime-and-courts/i--reopened-at-festus-after-cleanup-of-tanker-s/article_ea5888b9-59a0-5b70-96aa-abb674ecf558.html

13. *May 13, KVEW 42 Kennewick* – (Washington) **Apples spill down Highway 395.** Southbound lanes of Highway 395 in Kennewick were closed for about 4 hours May 13 while crews removed and cleared the scene of an accident involving a semi-truck that jackknifed and spilled barrels of apples onto the roadway.
Source: <http://www.kvewtv.com/article/2015/may/13/apples-spill-down-highway-395/>
14. *May 13, Philadelphia Inquirer* – (Pennsylvania) **Pa. Turnpike shut down in Montco as tractor-trailer overturns.** A stretch of the Pennsylvania Turnpike in Montgomery County was closed for several hours following a 4-vehicle accident involving an overturned semi-truck hauling 35,000 pounds of paper May 13. At least one person was injured and an inspector was dispatched to check the overpass for any structural damage.
Source: http://www.philly.com/philly/news/20150514_Pa_Turnpike_shut_down_in_Montco_as_tractor-trailer_overturns.html
15. *May 13, KRCR 7 Redding* – (California) **Highway 299E now open after fatal crash.** Highway 299E near Buzzard Roost Road in California was closed for approximately 7 hours May 13 while crews cleared the scene of an accident involving a semi-truck hauling fruit that rolled onto another vehicle while attempting to illegally pass another semi-truck, killing the driver of the vehicle.
Source: <http://www.krctrv.com/news/local/woman-killed-in-crash-highway-299e-to-be-closed-for-hours/32999890>

For another story, see item [29](#)

[\[Return to top\]](#)

Food and Agriculture Sector

16. *May 13, Associated Press* – (Iowa) **Iowa posts additional bird flu case on Sioux County egg farm.** The Iowa Department of Agriculture reported that an egg-laying farm in Sioux County with 238,000 chickens tested positive for bird flu, bringing the total number of cases in the county to 11 and 50 in the State. All of the infected chickens will be euthanized.
Source: <http://www.bnd.com/news/article20940579.html>
17. *May 13, KWVL 7 Waterloo* – (Iowa) **Thousands of pounds of milk spilled in Fayette County crash.** Forty-eight thousand pounds of milk were spilled May 12 when the driver of a milk truck lost control and rolled the vehicle into a ditch in Fayette County.
Source: <http://www.kwvl.com/story/29057223/2015/05/13/thousands-of-pounds-of-milk-spilled-in-fayette-county-crash>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

18. *May 14, Corpus Christi Caller-Times* – (Texas) **198,000 gallons of wastewater seep into creek.** An estimated 198,000 gallons of household wastewater spilled into La Volla Creek in Corpus Christi May 13 from a flooded sewage line near the Greenwood Wastewater Treatment Plant, prompting a precautionary boil advisory for area residents until the water supply is tested.

Source: http://www.caller.com/news/local-news/weather/198000-gallons-of-wastewater-seep-into-creek_10234019

For additional stories, see items [2](#) and [26](#)

[\[Return to top\]](#)

Healthcare and Public Health Sector

19. *May 13, Reuters* – (Florida) **CVS pays \$22 million to resolve Florida painkiller probe.** The U.S. Attorney's Office in Tampa announced May 13 that CVS Health Corp., will pay \$22 million in a settlement to resolve allegations that 2 of its pharmacies in central Florida sold painkillers that were not prescribed for legitimate medical purposes. Federal agents discovered that the pharmacies ordered about 3 million oxycodone pills in 2011 and ignored red flags that the prescriptions were not legitimate.

Source: <http://www.reuters.com/article/2015/05/13/us-cvs-health-settlement-idUSKBN0NY2O920150513>

For another story, see item [28](#)

[\[Return to top\]](#)

Government Facilities Sector

20. *May 13, WJBK 2 Detroit* – (Michigan) **Fog machine causes elementary school evacuation in Macomb Twp.** Over 30 students from Beck Centennial Elementary School in Macomb Township were hospitalized May 13 after suffering symptoms of nausea, headaches, and teary eyes during practice for a school musical caused by a fog machine containing chemicals. The school was evacuated and classes were canceled for the remainder of the day.

Source: <http://www.myfoxdetroit.com/story/29053620/fog-machine-causes-elementary-school-evacuation-in-macomb-twp>

21. *May 13, St. Louis Post-Dispatch* – (Missouri) **Wildfire contained in Mark Twain National Forest near Black, Mo.** Crews reached full containment May 13 of a wildfire that has burned 2,146 acres in the Mark Twain National Forest near Black,

Missouri. Firefighters will remain in the park to monitor the area until the fire is declared completely extinguished.

Source: http://www.stltoday.com/news/local/state-and-regional/wildfire-contained-in-mark-twain-national-forest-near-black/article_fec94726-50b8-5510-8faa-51c6cffaff42.html

22. *May 13, Times of Trenton* – (New Jersey) **Burlington City High School evacuated after bomb threat.** Students and staff at Burlington City High School in New Jersey were evacuated for 3 hours May 13 after the school received a bomb threat. Police cleared the scene after nothing suspicious was found.

Source:

http://www.nj.com/mercer/index.ssf/2015/05/burlington_city_high_school_evacuated_after_bomb_t.html

For another story, see item [2](#)

[\[Return to top\]](#)

Emergency Services Sector

Nothing to report

[\[Return to top\]](#)

Information Technology Sector

23. *May 14, Softpedia* – (International) **Cisco TelePresence vulnerable to unauthorized root access, denial of service.** Cisco reported two vulnerabilities in versions of its TelePresence TC and TE video conference products in which an attacker could exploit improper authentication protocols for internal services to bypass authentication and obtain root access on the system, and a flaw in the network drivers in which an attacker could use specially crafted internet protocol (IP) packets sent at a high rate to cause a denial-of-service (DoS) condition.

Source: <http://news.softpedia.com/news/Cisco-TelePresence-Vulnerable-to-Unauthorized-Root-Access-Denial-of-Service-481183.shtml>

24. *May 14, V3.co.uk* – (International) **APT17 DeputyDog hackers are pushing Blackcoffee malware using TechNet.** Research by FireEye revealed that the APT17 threat group used posts and profiles on the TechNet blog as a way to conceal their use of the Blackcoffee backdoor by embedding strings that the malware would decode to find and communicate with the malware's true command-and-control (C&C) server. The TechNet blog was not compromised and the operation was shut down, but FireEye warned that other groups may mimic the tactic.

Source: <http://www.v3.co.uk/v3-uk/news/2408533/apt17-deputydog-hackers-are-pushing-blackcoffee-malware-using-technet>

25. *May 13, Threatpost* – (International) **XSS, CSRF vulnerabilities identified in WSO2**

Identity Server. Researchers at SEC Consult discovered three cross-site scripting (XSS), cross-site request forgery (CSRF), and extensible markup language (XML) external injection vulnerabilities in version 5.0.0 of WSO2 Identity Server that could allow an attacker to take over a victim’s session, add arbitrary users to the server, or inject arbitrary XML entities.

Source: <https://threatpost.com/xss-csrf-vulnerabilities-identified-in-wso2-identity-server/112789>

26. *May 13, Securityweek* – (International) **Flaw found in OSISOft product deployed in critical infrastructure sectors.** OSISOft advised customers to mitigate an incorrect default permissions vulnerability in its PI Asset Framework (PI AF) in which an unauthorized remote attacker could leverage “Trusted Users” group status in some product installations to execute arbitrary structured query language (SQL) statements on the affected system, potentially leading to information disclosure, data tampering, privilege escalation, and/or denial-of-service (DoS) conditions.

Source: <http://www.securityweek.com/flaw-found-osisoft-product-deployed-critical-infrastructure-sectors>

For another story, see item [1](#)

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

27. *May 13, Allentown Morning Call* – (Pennsylvania) **TV service disrupted for 12,000 Service Electric customers.** About 12,000 Service Electric Cable TV & Communications Inc., customers in Leigh County lost television reception for approximately 2 hours May 13 after a satellite time server failed during routine database maintenance.

Source: <http://www.mcall.com/news/local/mc-service-electric-tv-outage-20150513-story.html>

[\[Return to top\]](#)

Commercial Facilities Sector

28. *May 14, Chester County Daily Local News* – (Pennsylvania) **Officials call fire a ‘total loss.’** Downingtown Police declared the North Park Plaza strip mall a total loss May 14 after 10 businesses and both floors of the mall were severely damaged in a May 12 fire. Preliminary reports estimated that the total amount of damage exceeded \$4 million, and

officials determined that the fire began in a florist shop.

Source: <http://www.dailylocal.com/general-news/20150513/officials-call-fire-a-total-loss>

29. *May 14, Monterey Herald* – (California) **Monterey Apple Store package that hospitalized 4 people contaminated at FedEx facility.** An Apple Store at the Del Monte Shopping Center in Monterey was evacuated and closed when four people including employees were hospitalized after reporting symptoms of nausea while picking up a package at the shopping center May 13. Officials reported that the clear liquid that sickened a dozen people was organic peroxide that spilled on the package at a FedEx distribution center before the package was delivered.
Source: <http://www.montereyherald.com/general-news/20150513/monterey-apple-store-package-that-hospitalized-4-people-was-contaminated-at-fedex-facility>
30. *May 13, Baltimore Sun* – (Maryland) **One estimate of business damage from Baltimore riot estimated at \$9M, total cost unknown.** The U.S. Small Business Administration announced May 13 that estimated damages to about 285 businesses in Baltimore following recent unrest in the city totaled about \$8.9 million. City and State officials are still investigating the total amount of damage which also included destruction to more than 30 homes, 150 vehicles, and 60 other structures.
Source: <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-damage-estimate-20150513-story.html>

[\[Return to top\]](#)

Dams Sector

See item [26](#)

[\[Return to top\]](#)



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

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.