



Daily Open Source Infrastructure Report 12 August 2015

Top Stories

- Authorities announced indictments against 9 Ukrainian hackers and securities traders in the U.S. and Ukraine August 11, alleging that the suspects conspired and made up to \$100 million by stealing confidential corporate press releases. – *Reuters* (See item [6](#))
- Crews worked to reopen a 34-mile stretch of Highway 89-A in Arizona after it was closed August 9 due to flood waters that washed mud and boulders across the highway. – *St. George News* (See item [13](#))
- The city of St. Petersburg, Florida, released 5.5 million gallons of treated sewage into Tampa Bay for 8 hours August 9 after excess rainfall overwhelmed the Southwest Water Reclamation Facility. – *Tampa Bay Times* (See item [16](#))
- Security researchers from IBM discovered an Android operating system (OS) “serialization vulnerability” related to Android’s OpenSSLX509Certificate class framework that an attacker could exploit. – *Securityweek* (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. *August 11, Scranton Times-Tribune* – (Pennsylvania) **More details emerge on alleged arson at Milford compressor station.** A natural gas compressor station for Columbia Pipeline Group in Milford Township in Pennsylvania, was the target of an alleged arson attack August 8 when a fire damaged the metal platform where a compression turbine sits, causing an estimated \$80,000 in damage. The station was under construction at the time of the fire and no gas was flowing through its pipes.
Source: <http://thetimes-tribune.com/news/more-details-emerge-on-alleged-arson-at-milford-compressor-station-1.1925417>
2. *August 10, Denver Post* – (Wyoming) **Wyoming oil facility explosion leaves 3 men injured; 1 flown to Greeley in critical condition.** An explosion and flash fire at an oil facility owned by Kaiser-Francis Oil Company in Wyoming injured 3 welders, 1 critically, August 10 after the workers may have hit a suspected natural gas line.
Source: http://www.denverpost.com/news/ci_28615751/wyoming-oil-facility-explosion-leaves-3-men-injured
3. *August 10, Columbia The State* – (South Carolina) **Unapproved coal ash dump will cost “green” company \$230,000 in state fine.** The South Carolina Department of Health and Environmental Control issued a \$230,000 fine to Sonoco for violating the State’s solid waste policy law by operating an unapproved coal ash dump in eastern South Carolina. The company found no evidence that the coal pile polluted groundwater or nearby waterways and a \$3 million cleanup project is expected to be completed by 2017.
Source: <http://www.thestate.com/news/local/article30671700.html>

For another story, see item [25](#)

Chemical Industry Sector

4. *August 10, Network World* – (International) **Cyber-physical attacks: Hacking a chemical plant.** Researchers with the European Network for Cyber Security and IOActive released their Damn Vulnerable Chemical Plant Process framework at Def Con 23 that stated ways in which a hacker could infiltrate a chemical plant, and taught defenders how to spot cyber-physical attacks. The report is the first open source framework based on two simulated chemical plants.
Source: <http://www.networkworld.com/article/2968432/microsoft-subnet/cyber-physical-attacks-hacking-a-chemical-plant.html>

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

5. *August 10, U.S. Department of Labor* – (Wisconsin) **Fire truck manufacturer exposes**

workers to amputation and fall hazards. The Occupational Safety and Health Administration cited FWD/Seagrave Apparatus of Clintonville August 10 with 1 willful, 1 serious, and 1 other-than-serious safety violations for not having guards in place, exposing workers to operating parts of press brakes, exposing workers to fall hazards, and for not having potable water available at work sites. Proposed penalties total \$77,000.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28542

Defense Industrial Base Sector

See item [25](#)

Financial Services Sector

6. *August 11, Reuters* – (International) **Nine charged in U.S. insider trading scheme involving hackers.** Authorities announced indictments against 9 Ukrainian hackers and securities traders in the U.S. and Ukraine August 11, alleging that the suspects conspired and made up to \$100 million by hacking into companies that publish news releases about publicly traded companies, and made trades using the information starting in February 2010. The U.S. Securities and Exchange Commission filed a related civil lawsuit alleging that the thefts generated over \$100 million in illegal profits, and the case is the first example of prosecution alleging the use of hacked inside information for securities fraud.
Source: <http://www.reuters.com/article/2015/08/11/cybersecurity-hacking-stocks-idUSL1N10M05H20150811>
7. *August 10, Reuters* – (National) **Citigroup in US\$13.5 mln settlement over defunct CSO hedge fund.** Citigroup Inc., announced an agreement August 10 to pay \$13.5 million to resolve allegations that the bank and its Alternative Investments affiliate deceived investors into staying in its Corporate Special Opportunities hedge fund, reporting that the fund's portfolio was sound before liquidating it and losing most of the investment funds.
Source: <http://www.reuters.com/article/2015/08/10/citigroup-prosiebensat-1-settlement-idUSL1N10L2OR20150810>
8. *August 10, Orange County Register* – (California) **Grand jury indicts retired LAPD cop suspected as 'Snowbird Bandit.'** A retired Los Angeles Police Department detective believed to be the robbery suspect dubbed the "Snowbird Bandit" was indicted the week of August 4, facing charges that he allegedly held up banks in Dana Point, Rancho Santa Margarita, Mission Viejo, and Ladera Ranch.
Source: <http://www.ocregister.com/articles/adair-676867-bank-santa.html>
9. *August 10, Reuters* – (National) **Guggenheim settles for \$20 mln over not disclosing loan -SEC.** The U.S. Securities and Exchange Commission (SEC) announced August 10 that Guggenheim Partners Investment Management LLC agreed to pay \$20

million to resolve allegations that company senior officials failed to disclose a \$50 million loan by a client to a senior executive to finance his personal investment in a corporate acquisition led by Guggenheim Partners LLC. The SEC also alleged that the company failed to enforce its code of ethics and improperly charged a client \$6.5 million in asset management fees it did not earn.

Source: <http://www.reuters.com/article/2015/08/10/sec-guggenheim-idUSL1N10L1GD20150810>

Transportation Systems Sector

10. *August 11, KNXV 15 Phoenix* – (Arizona) **DPS: Bus with 50 inmates involved in major crash on Interstate 8.** One westbound and one eastbound lane of Interstate 8 in Stanfield reopened after a portion of the interstate was closed for several hours August 11 due to an accident between a bus carrying inmates and a semi-truck hauling herbicide that left 2 staff members and 20 inmates injured.
Source: <http://www.abc15.com/news/region-central-southern-az/casa-grande/dps-bus-with-50-inmates-involved-in-major-crash-on-interstate-8>
11. *August 10, San Francisco Bay City News* – (California) **Woman arrested on suspicion of DUI following Highway 101 fatal crash in San Jose.** Southbound lanes of Highway 101 in San Jose were blocked for over 3 hours August 10 after a suspected drunk driver collided with another vehicle, leaving 1 person dead and 4 others injured.
Source: <http://abc7news.com/traffic/woman-arrested-for-dui-after-hwy-101-fatal-crash/917822/>
12. *August 10, KPCC 89.3 FM Pasadena* – (California) **Anza fire: 3 firefighters injured, highway closed in Riverside County blaze.** All lanes of Highway 74 east of the intersection with Highway 371 near Anza, California, were closed August 10 until further notice after a motor home fire spread to nearby vegetation.
Source: <http://www.scpr.org/news/2015/08/10/53698/brush-fire-forces-highway-closure-near-anza/>
13. *August 10, St. George News* – (Arizona) **‘Boulders the size of houses’; 34-mile road closure continues on Highway 89-A.** Crews worked to reopen a 34-mile stretch of Highway 89-A from milepost 545 to milepost 579 in Arizona after it was closed August 9 due to flood waters that washed mud and boulders across the highway.
Source: <http://www.stgeorgeutah.com/news/archive/2015/08/10/ccj-closure-89a>
14. *August 10, WCBS 2 New York City* – (New York) **Police: Man stole mail, burned off names from checks and cashed them.** A suspect wanted in connection with 18 mail thefts in East Harlem, Brooklyn, and the Bronx from January 2014 – May 2015 was identified by New York police August 10. The suspect allegedly removed mail from victims’ mailboxes and used chemicals to remove names from money orders, cashing the checks under falsified names.
Source: <http://newyork.cbslocal.com/2015/08/10/mail-check-theft/>

For another story, see item [31](#)

Food and Agriculture Sector

15. *August 10, Arizona Republic* – (Arizona) **Phoenix nut-roasting plant evacuated after oven catches on fire.** Phoenix officials reported that the Suntime nut-roasting plant evacuated about 25 employees August 10 after an oven overheated and caused smoke to fill the large commercial building. The fire was contained to the burner and one person suffered minor injuries.
Source: <http://www.azcentral.com/story/news/local/phoenix/breaking/2015/08/11/phoenix-fire-nut-roasting-plant/31438191/>

Water and Wastewater Systems Sector

16. *August 11, Tampa Bay Times* – (Florida) **Swamped by rains, St. Pete dumps treated sewage into Tampa Bay.** The city of St. Petersburg released 5.5 million gallons of treated sewage into Tampa Bay for 8 hours August 9 after excess rainfall overwhelmed the Southwest Water Reclamation Facility.
Source: <http://www.tampabay.com/news/overburdened-by-rains-st-pete-dumps-treated-sewage-into-tampa-bay/2240745>
17. *August 10, NBC News; Associated Press* – (Colorado) **State of emergency: Colorado wastewater leak far exceeds first estimates.** The governor of Colorado declared a state of emergency August 10 in response to an August 5 spill where a cleanup crew inadvertently breached a debris dam inside the Gold King Mine, spilling 3 million gallons of tainted wastewater into the Animas River.
Source: <http://www.nbcnews.com/news/us-news/colorado-mine-spill-toxic-wastewater-leak-far-exceeds-first-estimates-n407091>
18. *August 10, South Florida Sun Sentinel* – (Florida) **Large parts of Broward still under boil water order.** The city of Fort Lauderdale issued a boil water advisory for several municipalities and neighborhoods August 8 until further notice after an untreated water sample at one of south Florida's water source wells tested positive for E. coli bacteria.
Source: <http://www.sun-sentinel.com/news/fl-lauderdale-boil-water-order-20150809-story.html>

Healthcare and Public Health Sector

See items [25](#) and [32](#)

Government Facilities Sector

19. *August 11, KTAR 92.3 FM Glendale; Associated Press* – (Arizona) **Some Willow Fire evacuees allowed to return home.** Crews reached 40 percent containment August 11 of the nearly 7,000-acre Willow Fire burning in northwestern Arizona. Evacuation orders for several communities were lifted, and 11 structures have been burned down.
Source: <http://ktar.com/2015/08/10/wildfire-in-mohave-valley-forces-residents-to-evacuate/>

20. *August 11, Great Falls Tribune* – (Montana) **Three fires burn in Glacier National Park.** Crews reached 67 percent containment August 11 of the 4,311-acre Reynolds Creek Fire burning near Logan Pass, while additional fire crews worked to contain the 1,900-acre Thompson Fire burning in Glacier National Park.
Source: <http://www.usatoday.com/story/news/nation/2015/08/11/glacier-national-park-wildfire/31448371/>
21. *August 11, KRON 4 San Francisco* – (California) **Jerusalem Fire burns 12,000 acres in Lake County.** Firefighters worked to contain the Jerusalem Fire that burned 12,000 acres in Lake County by August 11, and prompted evacuation orders for a portion of the Jerusalem Valley areas.
Source: <http://kron4.com/2015/08/09/jerusalem-fire-burns-in-lake-county/>
22. *August 10, KGO 7 San Francisco* – (California) **Children injured after school bus crash on I-80 in Berkeley.** Nineteen children and adults on a Camp Kee Tov school bus were injured along with 4 other drivers due to a chain-reaction crash involving 8 vehicles on Interstate 80 in Berkeley August 10.
Source: <http://abc7news.com/traffic/children-injured-after-school-bus-crash-on-i-80-in-berkeley/918648/>
23. *August 10, Fresno Bee* – (California) **Fires burn in Sierra, Sequoia National Forests – one nears containment.** Crews reached 96 percent containment August 10 of the 5,871-acre Cabin Fire burning in Tulare County near the Golden Trout Wilderness. Firefighters also worked to contain the 4,754-acre Rough Fire burning in Fresno County in the Sierra National Forest.
Source: <http://www.fresnobee.com/news/local/article30672060.html>

For another story, see item [25](#)

Emergency Services Sector

24. *August 11, Natchez Democrat* – (Louisiana) **Four inmates escape Tensas Parish detention center.** Authorities are searching the Waterproof area for four inmates who escaped from the Tensas Parish Detention Center in Louisiana August 10 by allegedly exiting from a door in the housing area.
Source: <http://www.natchezdemocrat.com/2015/08/11/four-inmates-escape-tensas-parish-detention-center/>

For additional stories, see items [5](#), [10](#), [29](#), and [31](#)

Information Technology Sector

25. *August 11, Securityweek* – (International) **Darkhotel APT uses Hacking Team exploit to target specific systems.** Security researchers from Kaspersky Lab reported that the Darkhotel advanced persistent threat (APT) group recently started leveraging a Flash zero-day vulnerability revealed in the July Hacking Team Breach to target specific

systems, and that the group has been using a variety of techniques to attack defense industrial bases, energy policy makers, militaries, governments, electronics, pharmaceutical organizations, and medical providers in countries across Europe and Asia.

Source: <http://www.securityweek.com/darkhotel-apt-uses-hacking-team-exploit-target-specific-systems>

26. *August 11, Help Net Security* – (International) **Angler EK exploits recently patched IE bug to deliver ransomware.** Security researchers from FireEye discovered that the Angler exploit kit (EK) is exploiting a Microsoft Internet Explorer vulnerability uncovered in the July Hacking Team breach to deliver Cryptowall ransomware to affected systems.

Source: http://www.net-security.org/malware_news.php?id=3087

27. *August 11, IDG News Service* – (International) **Asprox botnet, a long-running nuisance, disappears.** Officials from Palo Alto networks found that the Asprox botnet was apparently shut down, after observers reported last seeing the botnet distributing the Kuluoz malware in 2014.

Source: <http://www.computerworld.com/article/2969338/security/asprox-botnet-a-longrunning-nuisance-disappears.html>

28. *August 11, Securityweek* – (International) **Serialization vulnerabilities put many Android devices at risk.** Security researchers from IBM discovered an Android operating system (OS) “serialization vulnerability” affecting versions 4.3 Jelly Bean through 5.1 Lollipop, related to Android’s OpenSSLX509Certificate class framework that an attacker could exploit for arbitrary code execution in applications and services, leading to privilege escalation, in which legitimate apps can be replaced with malicious apps that steal data, among other actions.

Source: <http://www.securityweek.com/serialization-vulnerabilities-put-many-android-devices-risk>

For additional stories, see items [4](#), [6](#), and [32](#)

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>

Communications Sector

29. *August 10, Okanogan Valley Gazette-Tribune* – (Washington) **CenturyLink customers experiencing internet, phone and 9-1-1 outage.** CenturyLink officials reported that about 3,000 customers were without 9-1-1, phone, and Internet services in Omak, Oroville, Pateros, Twisp, Winthrop, and surrounding areas in Washington August 10. Emergency 9-1-1 calls were rerouted while technicians worked to restore

services.

Source: <http://www.gazette-tribune.com/news/centurylink-customers-experiencing-internet-phone-and-911-outage/70562/>

30. *August 10, WROC 8 Rochester* – (New York) **Frontier outage frustrates customers.** Frontier officials reported that about 6,000 Rochester, New York, customers were without phone service from August 10 – 11 due to a faulty circuit board.
Source: <http://www.rochesterhomepage.net/story/d/story/frontier-outage-frustrates-customers/20865/AocgmX3i2U2jdAfHyMsw6A>

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

Commercial Facilities Sector

31. *August 11, NBC News* – (Missouri) **Ferguson demonstrations: Authorities declare state of emergency in St. Louis County.** Several businesses in the city of Ferguson were damaged by protestors August 10 commemorating the anniversary of an August 2014 incident, causing St. Louis County officials to declare a state of emergency. Police arrested more than 100 people when several protestors blocked traffic lanes on major highways and exchanged gunfire with officers.
Source: <http://www.nbcnews.com/storyline/michael-brown-shooting/protesters-arrested-while-marking-year-michael-browns-death-n407236>
32. *August 10, Wall Street Journal* – (National) **Fred's Inc. discloses cybersecurity breach.** Fred's Inc. officials reported August 10 that its two payment processing servers were compromised by thieves using malware designed to locate Track 2 data from March 23 – April 24 in which card numbers, expiration dates, and verification codes may have been used to create an unknown amount of counterfeit cards. The company found no evidence that customers' data were removed.
Source: <http://www.wsj.com/articles/freds-inc-discloses-cybersecurity-breach-1439248912>
33. *August 10, WPVI 6 Philadelphia* – (Pennsylvania) **Passengers evacuated from roller coast at Dorney Park.** Riders on the Talon roller coaster at Dorney Park in Allentown, Pennsylvania, were evacuated August 10 after a warning light appeared, halting the ride. All passengers were evacuated safely and no injuries were reported.
Source: <http://6abc.com/news/passengers-evacuated-from-roller-coaster-at-dorney-park/918752/>

Dams Sector

Nothing to report



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.