



Daily Open Source Infrastructure Report 02 February 2016

Top Stories

- The U.S. Food and Drug Administration (FDA) issued a ban January 29 on the import and sale of genetically engineered salmon until the FDA finalizes its labeling guidelines. – *Washington Post* (See item [11](#))
- Sheriff’s officials reported January 31 that all 3 inmates who escaped from the Men’s Central Jail in Orange County January 22 were back in custody after 1 turned himself in January 29 while the other 2 were arrested January 30. – *Associated Press* (See item [15](#))
- Wendy’s restaurant chain is investigating February 1 a possible data breach in their information technology (IT) networks after reports revealed that stores in the Midwest and East Coast may have had their customers’ cards illegally stolen and used in fraudulent transactions. – *Softpedia* (See item [21](#))
- Denver police reported January 30 that the second day of the 38th Annual Colorado Motorcycle Expo was cancelled after two motorcycle gangs allegedly opened fire, injured seven people, and killed one other. – *Denver Post* (See item [24](#))

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. *February 1, CNN* – (California) **Deadly California weather leaves 150,000 without power.** Heavy rains and strong winds in southern California January 31 left 1 person dead and knocked out electricity to more than 150,000 customers. Utility crews worked to restore service.
Source: <http://www.cnn.com/2016/02/01/us/california-weather/>
2. *January 29, KXMC 13 Minot* – (North Dakota) **Oil and salt water spill reported near Belfield.** The North Dakota Department of Health announced January 29 that about 300 barrels of an oil and a salt water mixture spilled from a pipeline January 28 at a White Rock Oil and Gas-owned site in Billings County. Officials reported to the site and are monitoring the incident.
Source: <http://www.kxnet.com/story/31095370/oil-and-salt-water-spill-reported-near-belfield>

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *January 31, U.S. Securities and Exchange Commission* – (National) **Barclays, Credit Suisse charged with dark pool violations.** The U.S. Securities and Exchange Commission announced January 31 that Barclays Capital Inc., and Credit Suisse Securities LLC agreed to pay a combined \$154.3 million to settle separate charges that the companies violated Federal securities laws while operating alternative trading systems known as dark pools and Credit Suisse's Light Pool after Barclays Capital Inc., misrepresented its efforts to police its dark pool, overrode its surveillance tool, and misled its subscribers about data feeds. Officials stated that Credit Suisse LLC failed to operate as advertised and did not comply with numerous regulatory requirements.
Source: <https://www.sec.gov/news/pressrelease/2016-16.html>
4. *January 29, U.S. Department of Justice* – (International) **Founder of Liberty Reserve pleads guilty to laundering more than \$250 million through his digital currency**

business. The founder of Liberty Reserve pleaded guilty January 29 to 1 count of conspiracy to commit money laundering after he laundered more than \$250 million through his underworld cyber-banking system which allowed over 5 million users to conduct anonymous and untraceable illegal transactions, and to distribute, store, and launder the proceeds of their crimes. In addition, charges against two co-conspirators and the company remain pending.

Source: <http://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital>

Transportation Systems Sector

5. *February 1, KTLA 5 Los Angeles* – (California) **Overtuned big rig forces closure of Southbound 15 Freeway in Cajon Pass.** Southbound lanes of 15 Freeway in the Cajon Pass was closed for several hours February 1 after a semi-truck collided with another vehicle and overturned.
Source: <http://ktla.com/2016/02/01/overtuned-big-rig-forces-closure-of-southbound-15-freeway-in-cajon-pass/>
6. *January 31, WXII 12 Winston-Salem* – (North Carolina) **Truck driver charged with DWI after cabbage spill on NC interstate.** Northbound Interstate 95 in Rocky Mountain was closed for several hours January 31 while crews worked to clean up hundreds of heads of cabbage that spilled from an overturned semi-truck. The truck driver was indicted with several charges including driving while impaired.
Source: <http://www.wxii12.com/news/Truck-driver-charged-with-DWI-after-cabbage-spill-on-NC-interstate/37749550>
7. *January 29, Associated Press* – (Texas) **Fiery crash on Texas highway leaves 2 dead.** A fatal two-vehicle crash shut down U.S. Highway 69 in Zavalla for approximately 11 hours January 29 after a semi-truck hauling crude oil was hit head on by another vehicle, killing both drivers and causing a fire to engulf both vehicles.
Source: <http://www.kwtx.com/content/news/Fiery-crash-on-Texas-highway-leaves-2-dead-366996261.html>

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

Food and Agriculture Sector

8. *January 30, U.S. Department of Agriculture* – (California) **The Noble Spoon recalls chicken and beef products produced without benefit of inspection.** The Food Safety and Inspection Service announced January 30 that The Noble Spoon issued a recall for approximately 289 pounds of its beef and chicken entree products sold in 8 variations after an investigation revealed the items were produced without the benefit of Federal inspection and do not have a mark of inspection. The products were distributed to retail locations in Marin and Sonoma counties in California.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-012-2016-release>

9. *January 29, Associated Press* – (Wisconsin) **Police recover another load of stolen cheese.** Authorities recovered 41,000 pounds of parmesan cheese worth \$90,000 January 28 in a Grand Chute, Wisconsin warehouse after it was stolen from a distributor in Marshfield January 15. Authorities have not disclosed if the case is related to a January 25 theft of \$70,000 worth of cheddar and other cheeses in Germantown.
Source: <http://www.nbc26.com/news/police-recover-another-load-of-stolen-cheese>
10. *January 29, U.S. Food and Drug Administration*– (National) **Garden of Life, LLC recalls Raw Meal Organic Shake & Meal products because of possible health risk.** Garden of Life LLC issued a voluntary nationwide recall January 29 for a limited quantity of its Raw Meal Organic Shake & Meal Chocolate, Original, Vanilla, and Vanilla Chai products sold in 30 varieties due to possible Salmonella Virchow contamination. The U.S. Food and Drug Administration is investigating illnesses linked to the products.
Source: <http://www.fda.gov/Safety/Recalls/ucm484027.htm>
11. *January 29, Washington Post* – (National) **FDA bans imports of genetically engineered salmon -- for now.** The U.S. Food and Drug Administration (FDA) issued a ban January 29 on the import and sale of genetically engineered salmon after the Federal government passed a bill which instructed regulators to forbid the sale of genetically engineered salmon until the FDA finalizes labeling guidelines.
Source: <https://www.washingtonpost.com/news/to-your-health/wp/2016/01/29/fda-bans-imports-of-genetically-engineered-salmon-for-now/>

For another story, see item [6](#)

Water and Wastewater Systems Sector

12. *February 1, WPTV 5 West Palm Beach* – (Florida) **Precautionary boil water notice for Vero Beach after power outage.** A precautionary boil water notice was issued for residents and businesses in Vero Beach, Florida January 31 after a transformer blew, causing approximately half the city to lose power and the loss of the city's water pressure. City officials reported that the notice will remain in effect until testing revealed the water was safe to drink.
Source: <http://www.wptv.com/news/region-indian-river-county/vero-beach/half-of-vero-beach-without-power>
13. *January 29, Bowie Patch* – (Maryland) **Water main break floods Bowie Street; repairs made.** A water main break in Bowie closed Mitchellville road for several hours while crews worked to fix the break that poured approximately 3 million gallons of water onto the road.
Source: <http://patch.com/maryland/bowie/water-main-break-floods-bowie-street-repairs-made-0>

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

14. *January 31, WTOP103.5 FM Washington, D.C.* – (Virginia) **2 Spotsylvania County schools closed due to power outage.** A January 31 power outage prompted the closure of Chancellor High and Chancellor Middle schools in Spotsylvania County February 1 while crews worked to restore service.

Source: <http://wtop.com/virginia/2016/01/2-spotsylvania-county-schools-closed-due-to-power-outage/>

Emergency Services Sector

15. *January 31, Associated Press* – (California) **2 remaining escapees returned to southern California jail.** The Orange County Sheriff's officials reported January 31 that all 3 inmates who escaped from the Men's Central Jail in California January 22 were back in custody after 1 turned himself in January 29 while the other 2 were arrested January 30 after a civilian reported seeing a parked vehicle similar to the one authorities were searching for. An investigation into their escape is ongoing.

Source: <http://www.foxnews.com/us/2016/01/31/2-remaining-escapees-returned-to-southern-california-jail.html>

16. *January 29, NBC News* – (National) **Hackers take aim at FOP, nation's largest police union.** The president of the Fraternal Order of Police (FOP) announced January 28 that its data systems were hacked by unidentified hackers, and that some information was posted on a social media platform online. The FOP's official Web site remained offline January 29 after authorities stated that all records were breached and that the data posted included bargaining contracts which are available on the open web.

Source: <http://www.nbcnews.com/tech/security/hackers-take-aim-fop-nation-s-largest-police-union-n507126>

Information Technology Sector

17. *February 1, SecurityWeek* – (International) **New Cross-Platform backdoors target Linux, Windows.** Security researchers from Kaspersky Lab reported that the Linux backdoor dubbed OLMYJUXM.exe was recently found infecting Window-based systems with new capabilities similar to the 32-bit Windows variant of the DropboxCache and uses the same filename templates to steal screenshots, audiocaptures, keylogs, and other arbitrary data by using the SetWindowsHook API for keylogger functionality to contact the command and control (C&C) server for commands, and sends a heartbeat signal via Hypertext Transfer Protocol (HTTP) similar to the Linux variant. Users were advised to have an anti-virus program enabled on their systems, to avoid opening emails from unknown sources, and to avoid installing applications from untrusted sources.

Source: <http://www.securityweek.com/new-cross-platform-backdoors-target-linux->

windows

18. *January 31, Softpedia* – (International) **OS X Security Compromised via the update process of many popular Mac apps.** Sparkle released version 0.13.1 that patched a flaw in its Sparkle Updater framework, used to disseminate app updates to Apple Mac users after a security researcher discovered that all the updated information was sent out in Hypertext Transfer Protocol (HTTP), which can allow an attacker to set up a Man-in-the-Middle (MitM) attack by intercepting update requests from the Appcast server and modifying the update message Extensible Markup Language (XML) request to add their own malicious code.
Source: <http://news.softpedia.com/news/os-x-security-compromised-via-the-update-process-of-many-popular-mac-apps-499666.shtml>

19. *January 30, Softpedia* – (International) **iOS app hot patching reveals a gaping security hole in Apple's Walled Garden.** Security researchers from FireEye discovered a process flaw in how Apple's iOS developers patch their applications using the JSPatch library after researchers found they could deliver malicious instructions to test application, such as loading sensitive local iOS application program interfaces (APIs) and using them to access personal information, which was an unapproved function. The JSPatch engine translates the JavaScript code into Objective-C, which can allow any type of iOS exploit to be executed.
Source: <http://news.softpedia.com/news/ios-app-hot-patching-reveals-a-gaping-security-hole-in-apple-s-walled-garden-499654.shtml>

20. *January 29, SecurityWeek* – (International) **Firefox warns of password requests over HTTP.** Firefox released updates to its Mozilla browser, starting with Firefox DevEdition 46 that warned users when passwords were requested over non-secure connections and advised users to only provide passwords on secure connections such as Hypertext Transfer Protocol (HTTP) after a security researcher discovered the non-secure Web sites could be manipulated by a Man-in-the-Middle (MitM) attacker. The new Mozilla feature will check each web page against the algorithm in the World Wide Web Consortium's (W3C) Secure Contexts Specification to determine whether the page is secure or not, and will warn security developers if the page is not secure.
Source: <http://www.securityweek.com/firefox-warns-password-requests-over-http>

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

Nothing to report

Commercial Facilities Sector

21. *February 1, Softpedia* – (National) **Wendy’s restaurant chain is investigating data breach. Officials from** Wendy’s fast food restaurant chain is investigating February 1 a possible data breach in their information technology (IT) networks after reports from the company’s financial sector revealed that stores in the Midwest and East Coast may have had their customers’ cards illegally stolen and used in fraudulent transactions outside the restaurant chain. Officials reported that they are unsure how many stores were affected.
Source: <http://news.softpedia.com/news/wendy-s-restaurant-chain-is-investigating-data-breach-499704.shtml>
22. *February 1, KTLA 5 Los Angeles* – (California) **Fire tears through old brick commercial building in Glassell Park; arson section investigating.** The Los Angeles Fire Department reported that about 150 firefighters were deployed February 1 to extinguish a fire at a commercial building that housed several businesses for nearly 2 hours. The cause of the incident was not determined and the total amount of damages was not disclosed.
Source: <http://ktla.com/2016/02/01/firefighters-respond-to-blaze-in-glassell-park/>
23. *January 31, Columbus Dispatch* – (Ohio) **Fire damages Buddhist temple in Franklinton; arson suspected.** The Karma Thegsum Choling temple in Franklinton, Ohio, sustained extensive damage January 31 after fire officials remained onsite for more than 2 hours containing the incident. An investigation is ongoing to determine the cause of the fire and the total amount of damages was unknown.
Source: <http://www.dispatch.com/content/stories/local/2016/01/31/0131-arson-suspected-in-buddhist-temple-fire.html>
24. *January 30, Denver Post* – (Colorado) **Denver cancels second day of motorcycle expo after shooting kills one.** The Denver Police Department reported January 30 that the second day of the 38th Annual Colorado Motorcycle Expo was cancelled due to safety concerns after two motorcycle gangs allegedly shot four people, injured two people, and killed one other at the conference. Officials believe there was more than one shooter and are investigating the incident.
Source: http://www.denverpost.com/news/ci_29453858/shootings-stabbings-reported-at-denver-coliseum

For another story, see item [12](#)

Dams Sector

25. *February 1, KCRA 3 Sacramento* – (California) **Ice dam causes flooding in Nevada County.** The Nevada County Office of Emergency Services reported January 31 that high water forced the closure of Soda Springs Road and forced the closure of the community after ice dams built up in the South Fork of the Yuba River, prompting crews to utilize heavy machinery to remove the ice dam.
Source: <http://www.kcra.com/news/local-news/news-sierra/flooding-cuts-off-nevada->



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.