# Daily Open Source Infrastructure Report
# 22 July 2016

## Top Stories

- Federal officials reached a $176 million settlement with Enbridge Energy Partners July 20 following the release of at least 843,000 gallons of crude oil into the Kalamazoo River in Michigan in July 2010. – *Associated Press* (See item 2)
- Two men were arrested in Corona, California, July 16 after authorities found about 150 counterfeit credit cards, an encoding machine, and several counterfeit IDs, among other illicit materials in the duo's apartment. – *San Francisco Bay City News* (See item 5)
- Southwest Airlines reported July 20 that up to 700 flights across its network were canceled and delayed due to multiple performance issues with its technology systems following an outage. – *IDG News Service* (See item 7)
- Federal officials issued a public health alert July 21 after the Washington State Department of Health reported confirmed cases of Salmonella potentially linked to the use and consumption of Kapowsin Meats Inc.'s, whole hog roasters prepared for barbecue. – *U.S. Department of Agriculture* (See item 12)

**Fast Jump Menu**

## Energy Sector

1. *July 21, Minneapolis Star Tribune* – (Minnesota, Wisconsin) **Storms leave thousands without power in Duluth area, Twin Cities.** Severe storms that moved through northeastern Minnesota and northwestern Wisconsin July 21 knocked out power to approximately 55,000 customers following strong winds that took down power lines.
Source: http://www.startribune.com/storms-leave-thousands-without-power-in-duluth-area-twin-cities/387774671/

2. *July 20, Associated Press* – (National) **Enbridge reaches $176M agreement for 2010 Michigan oil spill.** The U.S. Department of Justice and U.S. Environmental Protection Agency reached a $176 million settlement with Enbridge Energy Partners July 20 following the release of at least 843,000 gallons of crude oil into the Kalamazoo River in Michigan in July 2010. Under the settlement, Enbridge must replace nearly 300 miles of pipeline between Neche, North Dakota, and Superior, Wisconsin, as well as develop measures to prevent future spills, detect leaks, and prepare for emergencies across Enbridge's Lakehead network that extends more than 2,000 miles across 7 States, among other requirements.
Source: http://abcnews.go.com/International/wireStory/enbridge-reaches-176m-agreement-2010-michigan-oil-spill-40754722

3. *July 20, Associated Press* – (North Dakota) **Over 10K gallons of oil, produced water spill near Keene.** The North Dakota Industrial Commission, Oil and Gas Division reported July 20 that more than 10,000 gallons of an oil and produced water mixture spilled at a well site in McKenzie County following a piping connection leak. Officials stated over 9,500 gallons of the mixture have been recovered.
Source: http://www.fairfieldcitizenonline.com/news/article/Over-10K-gallons-of-oil-produced-water-spill-8399360.php

## 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

4. *July 20, KRDO 13 Colorado Springs* – (Colorado) **"Dum-Dum Bandit" robs 3 Colorado banks in 30 days.** The FBI is searching July 20 for a man dubbed the "Dum-Dum" Bandit who is suspected of robbing three banks in Denver since June, including a U.S. Bank branch July 19.
Source: http://www.krdo.com/news/dumdum-bandit-robs-3-colorado-banks-in-30-days/40807262

5. *July 20, San Francisco Bay City News* – (California) **Police seize 150 credit cards, IDs in counterfeit bust.** Two men were arrested in Corona, California, July 16 after authorities found about 150 counterfeit credit cards, numerous counterfeit IDs, and an encoding machine, among other illicit materials in the duo's apartment after police received information regarding the illegal activities in May. Officials said the duo used the counterfeit cards to make fraudulent purchases in Los Angeles, Orange, and Riverside counties.
Source: http://patch.com/california/temecula/police-seize-150-fake-credit-cards-ids-counterfeit-bust

## Transportation Systems Sector

6. *July 21, Knoxville News Sentinel* – (Tennessee) **Maryville College grad, Virginia trucker killed in I-40 crash near downtown Knoxville.** All lanes of Interstate 40 in Knoxville, Tennessee, were closed for 8 hours July 20 while crews worked to clear the wreckage from a head-on collision that left two people dead.
Source: http://www.knoxnews.com/news/local/tdot-crash-shuts-down-i-40-near-downtown-knoxville-380e327b-2c24-6f29-e053-0100007f506f-387593011.html

7. *July 20, IDG News Service* – (National) **Southwest Airlines delay flights after computer issues.** Southwest Airlines reported July 20 that up to 700 flights across its network were canceled and delayed due to multiple performance issues with its technology systems following an outage. Normal operations were expected to be restored July 21.
Source: http://www.networkworld.com/article/3098307/southwest-airlines-delays-flights-after-computer-issues.html#jump

8. *July 20, WBAY 2 Green Bay* – (Wisconsin) **Green Bay bridges reopen after train is moved.** Traffic was blocked for approximately 2 hours on the Walnut Street and Main Street bridge crossings in Green Bay, Wisconsin, July 20 after a Canadian National Railway Company's locomotive derailed, preventing a second train that was blocking the bridge crossings from moving.
Source: http://wbay.com/2016/07/20/derailed-train-blocks-downtown-green-bay-traffic/

9. *July 20, Kennewick Tri-City Herald* – (Washington) **Bridge trouble closes Little Goose Dam to vehicles.** The Little Goose Lock and Dam across Snake River in Columbia County, Washington, was temporarily closed to vehicle traffic July 20 as

crews began repairs on the bridge after maintenance staff discovered mechanical issues with the motor that operates the bridge.
Source: http://www.tri-cityherald.com/news/local/article90924102.html

10. *July 20, MauiNow.com* – (Hawaii) **Honoapi‘ilani HAZMAT spill caused by broken hydraulic line on garbage truck.** Honoapi‘ilani Highway in Honokowai, Hawaii, was closed for more than 3 hours July 20 after a semi-truck burst a hydraulic line and spilled about 35 gallons of hydraulic fluid along the highway. HAZMAT crews worked to clean up the spill.
Source: http://mauinow.com/2016/07/20/honoapiilani-hazmat-spill-caused-by-broken-hydraulic-line-on-garbage-truck/

For another story, see item **2**

## Food and Agriculture Sector

11. *July 21, Food Safety News* – (National) **More than 600 sick in 45 States because of poultry pets.** The U.S. Centers for Disease Control and Prevention announced the week of July 18 that a total of 611 people in 45 States have been sickened by 8 separate outbreaks of Salmonella since January. Officials stated the outbreaks are linked to contact with live poultry and backyard flocks.
Source: http://www.foodsafetynews.com/2016/07/more-than-600-sick-in-45-states-because-of-poultry-pets/#.V5C5EvkrKUk

12. *July 21, U.S. Department of Agriculture* – (National) **FSIS issues public health alert for pork product due to possible Salmonella contamination.** The U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) issued a public health alert July 21 after the Washington State Department of Health notified the FSIS of confirmed case patients involved in a Salmonella outbreak potentially linked to the use and consumption of Kapowsin Meats Inc.’s, whole hog roasters prepared for barbecue after a traceback investigation found three of the case-patients had consumed the pork products. FSIS personnel are working to remove the products from commerce.
Source: http://www.fsis.usda.gov/wps/portal/fsis/newsroom/news-releases-statements-and-transcripts/news-release-archives-by-year/archive/2016/pha-072016

13. *July 20, U.S. Food and Drug Administration* – (National) **Krispak, Inc., issues allergy alert on undeclared tree nuts – pecans in GFS Honey Roasted Peanuts received from supplier Trophy Nut Co.** Krispak, Inc., issued a recall July 20 for a small quantity of its Gordon Food Service (GFS) Honey Roasted Peanuts products sold in 38-ounce containers due to mislabeling and undeclared pecans after the company discovered pecans were mixed in with the honey roasted peanuts the firm purchased from its supplier, Trophy Nut Co. No illnesses have been reported and the products were shipped to Gordon Food Service distribution centers in Florida, Massachusetts, Michigan, Ohio, and Pennsylvania.
Source: http://www.fda.gov/Safety/Recalls/ucm512354.htm

14. *July 20, San Francisco Chronicle* – (California) **500 tons of hay burn at Petaluma**

**dairy farm fire.** Authorities are investigating the cause of a July 20 fire at Moreda Valley Dairy in Petaluma, California, that burned through about 500 tons of alfalfa hay. No injuries were reported.
Source: http://www.sfgate.com/bayarea/article/500-tons-of-hay-burn-at-Petaluma-dairy-farm-fire-8399162.php

## Water and Wastewater Systems Sector

Nothing to report

## Healthcare and Public Health Sector

Nothing to report

## Government Facilities Sector

15. *July 21, KTVB 7 Boise* – (Idaho) **BLM: Wildfire near Hilltop Station now 60 percent contained.** Crews reached 60 percent containment July 21 of the 4,500-acre wildfire burning near Hilltop Station in Idaho. Officials closed Rocky Canyon road, Highland Valley road, and select trails in the area as a precaution.
Source: http://www.ktvb.com/news/local/blm-responding-to-wildfire-near-hilltop-station/277072390

16. *July 20, Columbia State* – (South Carolina) **Animals killed, building total loss in Huntington Beach State Park Nature Center fire.** The Nature Center at Huntington Beach State Park was considered a total loss July 20 following a fire that left all the animals inside dead. The cause of the fire remains under investigation.
Source: http://www.thestate.com/news/state/south-carolina/article90740912.html

17. *July 19, KSTU 13 Salt Lake City* – (Utah) **1,500-acre fire burning near ranches, historic Pony Express trial in Juab County.** Crews were working July 19 to contain the 1,500-acre Choke Cherry Fire burning in Juab County, Utah.
Source: http://fox13now.com/2016/07/19/1500-acre-fire-burning-near-ranches-historic-pony-express-trail-in-juab-county/

## Emergency Services Sector

Nothing to report

## Information Technology Sector

18. *July 21, Help Net Security* – (International) **Vulnerabilities affecting SAP HANA and SAP Trex put 10,000 customers at risk.** Onapsis released security advisories reporting on vulnerabilities in SAP High-Performance Analytic Appliance (HANA) and SAP Trex including a critical risk brute force attack affecting SAP HANA that could allow an attacker to gain unrestricted access to business information, and a critical risk remote command execution flaw affecting SAP Trex that could allow an

unauthenticated attacker to modify arbitrary database information, among other vulnerabilities. Researchers from Onapsis reported the flaws pose a risk to over 10,000 SAP customers running different versions of SAP HANA.
Source: https://www.helpnetsecurity.com/2016/07/21/sap-vulnerabilities/

19. *July 21, Help Net Security* – (International) **Cisco plugs critical flaw in data center operations management solution.** Cisco patched a critical vulnerability affecting its Unified Computing System (UCS) Performance Manager software's Web framework after a researcher from the Adidas Group discovered that an attacker could exploit the vulnerability by sending crafted Hypertext Transfer Protocol Secure (HTTP) GET requests to an affected system, allowing the attacker to execute arbitrary commands with root user privileges.
Source: https://www.helpnetsecurity.com/2016/07/21/data-center-operations-cisco/

20. *July 21, SecurityWeek* – (International) **Chrome 52 patches 48 vulnerabilities.** Google released Chrome 52 patching 48 security flaws including 11 high risk flaws and 6 medium severity flaws after external researchers found a high risk sandbox escape flaw in Pepper Plugin application programming interface (PPAPI), a high risk uniform resource locator (URL) spoofing on iOS, a use-after-free in Extensions, and a heap-buffer-overflow issue affecting sfntly, among other vulnerabilities.
Source: http://www.securityweek.com/chrome-52-patches-48-vulnerabilities

21. *July 20, Softpedia* – (International) **Backdoor account found in Dell network security products.** Researchers from Digital Defense, Inc., (DDI) released patches addressing six serious security flaws affecting the Dell SonicWALL Global Management System (GMS) after discovering the equipment had a hidden account that could be exploited to add non-administrative users via the command-line interface (CLI) Client, thereby elevating an attacker's privilege and allowing the malicious actor full control of the GMS interface and all attached SonicWALL appliances. DDI researchers also discovered two unauthenticated root command injections that lead to remote code execution (RCE) with root privileges on Dell equipment, among other vulnerabilities.
Source: http://news.softpedia.com/news/backdoor-found-in-dell-network-security-products-506477.shtml

22. *July 20, SecurityWeek* – (International) **CrypMIC ransomware emerges as CryptXXX copycat.** Trend Micro security researchers discovered a ransomware dubbed CrypMIC was mimicking the CryptXXX ransomware family, in that it exploits the Neurtino exploit kit (EK) to distribute the malware, utilizes the same ransom note and payment site, and employs a custom protocol via transmission control protocol (TCP) Port 443 to communicate with its command and control (C&C) servers, among other similarities. Researchers reported that the source code and capabilities of the two families are different after finding the CrypMIC ransomware cannot harvest credentials and related information from the affected device, as it does not download and execute an information-stealing module on its process memory.
Source: http://www.securityweek.com/crypmic-ransomware-emerges-cryptxxx-copycat

23. *July 20, Threatpost* – (International) **SoakSoak botnet pushing Neutrino exploit kit and CryptXXX ransomware.** Invincea researchers reported a surge in CryptXXX ransomware infections targeting popular Web sites running the Revslider slideshow plugin for Wordpress after discovering the SoakSoak botnet was delivering the CryptXXX ransomware via business Web sites that were compromised to redirect to the Neutrino exploit kit (EK).
Source: https://threatpost.com/soaksoak-botnet-pushing-neutrino-exploit-kit-and-cryptxxx-ransomware/119379/

**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

24. *July 21, KGO 7 San Francisco* – (California) **Crews investigating after Millbrae Community Center destroyed by 4-alarm fire.** The Millbrae Community Center in Millbrae, California, was considered a total loss following a four-alarm fire July 21. No injuries were reported and the cause of the fire remains under investigation.
Source: http://abc7news.com/news/firefighters-battling-4-alarm-fire-at-millbrae-community-center/1436384/

## Dams Sector

25. *July 20, MLive.com* – (Michigan) **160-year-old dam comes down along Grand River.** Crews began demolishing the 160-year-old Lyons Dam on the Grand River in Lyons, Michigan, July 20 as part of an emergency repair operation that began in June 2016 after the west edge of the dam failed and began eroding.
Source: http://www.mlive.com/business/west-michigan/index.ssf/2016/07/160-year-old_dam_comes_down_on.html


## 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.