



Daily Open Source Infrastructure Report 27 October 2016

Top Stories

- Subaru issued a recall October 26 for over 100,000 of its model years 2007 – 2014 vehicles in select makes due to a faulty relay that controls a secondary air injection pump, which can cause the pump to run continuously and overheat. – *Associated Press* (See item [2](#))
- A Federal judge approved October 25 a nearly \$15 billion settlement with the Federal Government, the State of California, and the Volkswagen Group after the automaker admitted that it rigged 11 million vehicles with software designed to cheat emissions standards. – *USA Today* (See item [3](#))
- Life Care Centers of America Inc. and its owner agreed October 24 to pay \$145 million after the company submitted false claims to Medicare and Tricare for rehabilitation therapy services that were medically unnecessary. – *U.S. Department of Justice* (See item [11](#))
- A therapist at JH Physical Therapy in Walnut, California, pleaded guilty October 24 for his role in a \$2.6 million Medicare fraud scheme. – *U.S. Department of Justice* (See item [12](#))

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. *October 25, Durango Herald* – (Colorado) **City council weighs in on gas outage that hits hundreds.** Around 750 Atmos Energy Corporation customers in Durango, Colorado, suffered a natural gas service outage for several hours October 25 – October 26 after air entered a pipeline during ongoing maintenance work.

Source:

<http://www.durangoherald.com/article/20161025/NEWS01/161029600/0/NEWS01/Gas-outage-affects-hundreds-in-Durango>

For additional stories, see items [3](#), [5](#), and [15](#)

Chemical Industry Sector

See item [15](#)

Nuclear Reactors, Materials, and Waste Sector

See item [15](#)

Critical Manufacturing Sector

2. *October 26, Associated Press* – (National) **Subaru recalls 4 models; turbo air pump can catch fire.** Subaru issued a recall October 26 for over 100,000 of its model years 2007 – 2014 vehicles in select makes equipped with turbocharged engines sold in the U.S. due to a faulty relay that controls a secondary air injection pump, which can cause the pump to run continuously and overheat, thereby increasing the risk of a fire.
Source: <http://www.foxbusiness.com/markets/2016/10/26/subaru-recalls-4-models-turbo-air-pump-can-catch-fire.html>
3. *October 25, USA Today* – (National) **Judge approves \$15B Volkswagen settlement.** A Federal judge approved October 25 a nearly \$15 billion settlement with the Federal Government, the State of California, and the Volkswagen Group after the automaker admitted that it rigged 11 million vehicles internationally with software designed to cheat emissions standards. As part of the settlement, Volkswagen must pay \$2.7 billion for environmental mitigation and initiate a vehicle buyback program which offers 475,000 Volkswagen owners in the U.S. the choice between a buyback or a free fix and compensation, among other requirements.
Source: <http://www.usatoday.com/story/money/cars/2016/10/25/volkswagen-settlement-approved/92719174/>
4. *October 24, Threatpost* – (International) **Rowhammer vulnerability comes to Android.** Security researchers discovered attackers could employ the Rowhammer attack to exploit an Android vulnerability, dubbed Drammer in order to achieve root-level access on millions of Android handsets including Nexus, Samsung, LG, and Motorola due to a hardware flaw in the Dynamic Random Access Memory (DRAM) memory modules. Researchers reported that Rowhammer targets rows of memory cells

in DRAM devices to cause cells to flip from one state to another, thereby allowing for memory manipulation.

Source: <https://threatpost.com/rowhammer-vulnerability-comes-to-android/121480/>

For additional stories, see items [15](#) and [16](#)

Defense Industrial Base Sector

See item [15](#)

Financial Services Sector

Nothing to report

Transportation Systems Sector

5. *October 26, Belleville News-Democrat* – (Illinois) **Power restored for most after train derails in Belleville.** Eleven coal cars of a Norfolk Southern train derailed October 25 in Belleville, Illinois, knocking out power to more than 500 area residents for several hours, forcing the closure of several roads, and prompting officials to cancel classes at Althoff Catholic High School. No injuries were reported and crews were working to repair the downed power lines and clean up the debris.
Source: <http://www.bnd.com/news/local/article110516152.html>
6. *October 26, Provo Daily Herald* – (Utah) **American Fork man killed in crash at mouth of Spanish Fork Canyon.** U.S. Highway 6 near the mouth of Spanish Fork Canyon in Spanish Fork, Utah, was closed for several hours October 25 after a vehicle drifted across the center line and struck a semi-truck head-on. One person was killed and the cause of the crash remains under investigation.
Source: http://www.heraldextra.com/news/local/south/spanish-fork/one-confirmed-dead-in-crash-at-mouth-of-spanish-fork/article_5461ee2d-9034-531d-b977-fc6f19f8700f.html
7. *October 25, KSBY 6 San Luis Obispo* – (California) **CHP investigating fatal head-on crash on Highway 166.** Highway 166 near Cuyama, California, was closed for several hours October 25 following a head-on collision involving a semi-truck and another vehicle that killed 1 person.
Source: <http://www.ksby.com/story/33475138/chp-investigating-fatal-head-on-crash-on-highway-166>

Food and Agriculture Sector

8. *October 25, U.S. Department of Agriculture* – (National) **Crider Inc. recalls canned organic roasted chicken breast due to possible foreign matter contamination.** Crider Inc. issued a recall October 25 for approximately 5,610 pounds of its “Wild Planet Organic Roasted Chicken Breast – 100% Chicken Breast & Sea Salt – No Liquids Added” products sold in 5-ounce cans due to potential contamination with

foreign materials after a distributor received 2 consumer complaints regarding foreign matter in the products. One potential injury has been reported and the products were shipped to multiple distributors for further circulation.

Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-100-2016-release>

Water and Wastewater Systems Sector

9. *October 25, Danbury Daily Voice* – (Connecticut) **Danbury to draw from Lake Kenosia as state declares water supply emergency.** The commissioner of the Connecticut Department of Public Health signed an order October 24 declaring a 30-day public water supply emergency for Danbury that permits the city to draw its water supply from Lake Kenosia due to drought conditions that are straining several reservoirs across the State. As part of the emergency declaration, the city must continue mandatory outdoor watering bans, provide weekly public notifications on water supplies for the impacted towns, and conduct a water audit of its top 20 largest water users, among other mandates.

Source: <http://danbury.dailyvoice.com/news/danbury-to-draw-from-lake-kenosia-as-state-declares-water-supply-emergency/687061/>

Healthcare and Public Health Sector

10. *October 25, U.S. Environmental Protection Agency* – (Puerto Rico) **EPA fines Pfizer in Puerto Rico for not disclosing chemical information.** The U.S. Environmental Protection Agency (EPA) announced October 25 a \$190,000 fine against Pfizer Pharmaceuticals LLC to resolve alleged Federal Clean Air Act violations after a 2014 inspection at the company's Barceloneta, Puerto Rico plant found that regulated chemicals, including methylamine and ammonia, were used in processes at the facility in excess of regulatory limits and without proper disclosure to the EPA.
Source: <https://www.epa.gov/newsreleases/epa-fines-pfizer-puerto-rico-not-disclosing-chemical-information>
11. *October 24, U.S. Department of Justice* – (National) **Life Care Centers of America Inc. agrees to pay \$145 million to resolve False Claims Act allegations relating to the provision of medically unnecessary rehabilitation therapy services.** Life Care Centers of America Inc. and its owner agreed October 24 to pay \$145 million to resolve alleged False Claims Act violations after the company submitted false claims to Medicare and Tricare for rehabilitation therapy services that were unreasonable and medically unnecessary, and sought to keep patients at the facilities longer than necessary in order to increase its Medicare and Tricare billings for reimbursement between January 2006 and February 2013.
Source: <https://www.justice.gov/opa/pr/life-care-centers-america-inc-agrees-pay-145-million-resolve-false-claims-act-allegations>
12. *October 24, U.S. Department of Justice* – (California) **Licensed occupational therapist pleads guilty to \$2.6 million Medicare fraud conspiracy.** A licensed occupational therapist at JH Physical Therapy in Walnut, California, pleaded guilty

October 24 for his role in a \$2.6 million Medicare fraud scheme where he and co-conspirators fraudulently billed Medicare for occupational therapy services that were not provided to Medicare beneficiaries between October 2009 and December 2012. The charges state that of the roughly \$2.6 million billed in false claims, Medicare paid the group more than \$1.8 million.

Source: <https://www.justice.gov/opa/pr/licensed-occupational-therapist-pleads-guilty-26-million-medicare-fraud-conspiracy>

Government Facilities Sector

13. *October 25, Portland Oregonian* – (Oregon) **\$300,000 in damage to new Roosevelt High School building blamed on vandalism.** Roosevelt High School in Portland, Oregon, sustained an estimated \$300,000 in damage after an act of vandalism flooded 6 classrooms and 6 bathrooms October 15. School officials stated the damaged rooms will be unusable for several weeks while repairs are completed.

Source:

http://www.oregonlive.com/education/index.ssf/2016/10/300000_in_damage_to_new_roosevelt.html

14. *October 24, WLBY 2 Bangor* – (Maine) **Ellsworth schools closed while police search for Sunday's suspected shooter.** Officials closed all Ellsworth School Department schools in Ellsworth, Maine, October 24 while authorities searched for a man suspected of firing a gun at a nearby apartment complex. No injuries were reported.

Source: <http://www.wlby2.com/news/local/ellsworth-schools-closed-while-police-search-for-sundays-shooter/340443730>

For another story, see item [5](#)

Emergency Services Sector

Nothing to report

Information Technology Sector

15. *October 26, SecurityWeek* – (International) **Data leaked by pagers useful for critical infrastructure attacks.** Trend Micro security researchers reported that pagers used in industrial control systems (ICS) were susceptible to targeted attacks, as the messages sent to the devices are unencrypted, thereby allowing hackers to easily intercept the information regarding the operation of a facility and potentially use that information in a targeted social engineering attack against the company. Trend Micro found that messages sent by nuclear plants, chemical facilities, defense contractors, HVAC manufacturers, and power substations via pagers leaked potentially sensitive information.

Source: <http://www.securityweek.com/data-leaked-pagers-useful-critical-infrastructure-attacks>

16. *October 26, Threatpost* – (International) **Major vulnerability found in Schneider**

Electric Unity Pro. Indegy security researchers discovered that Schneider Electric's Unity Pro PLC Simulator component of its Unity Pro software was plagued with a critical vulnerability that could allow hackers to remotely execute code on industrial networks if the Internet Protocol (IP) address of the Microsoft Windows PC running the software is accessible to the Internet, as the software allows any user to remotely run code directly on any device with Unity Pro installed. The flaw, which affects all versions prior to and including 11.1, could allow attackers to impact the production process within an industrial control system (ICS) physical environment.
Source: <https://threatpost.com/major-vulnerability-found-in-schneider-electric-unity-pro/121550/>

17. *October 25, SecurityWeek* – (International) **Apple patches multiple flaws in iOS, macOS, Sierra, Safari.** Apple released version 10.1 for its mobile operating system (iOS) patching 13 vulnerabilities affecting components such as FaceTime, Kernel, Security, and WebKit, among others, which could allow an attacker to run arbitrary code on the affected devices, leak sensitive user information, and execute arbitrary code with root privileges, among other malicious actions. Apple also released Sierra version 10.12.1 resolving 16 vulnerabilities that could result in privilege escalation, denial-of-service (DoS) conditions, process memory disclosure, and arbitrary code execution, as well as Safari version 10.0.1 resolving 3 vulnerabilities affecting WebKit, among other patches.

Source: <http://www.securityweek.com/apple-patches-multiple-flaws-ios-macos-sierra-safari>

18. *October 25, SecurityWeek* – (International) **Critical vulnerabilities patched in Joomla.** Joomla released version 3.6.4 addressing two critical account creation vulnerabilities in its content management system (CMS) versions 3.4.4 through 3.6.3, including a flaw that could allow an attacker to register on a Website even if registration has been disabled due to inadequate checks. The second vulnerability can be exploited by users to register on a Website with elevated privileges due to an incorrect use of unfiltered data.

Source: <http://www.securityweek.com/critical-vulnerabilities-patched-joomla>

For another story, see item [4](#)

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

Nothing to report

Dams Sector

19. *October 25, WTVD 11 Durham* – (North Carolina) **State orders Woodlake Dam owner to breach it and drain water.** North Carolina officials reported October 24 that the owners of the Woodlake Dam in Moore County are required to intentionally breach the dam and drain all the lake's water due to concerns that the dam could fail after it leaked during Hurricane Matthew, forcing dozens of residents to evacuate. Engineers expect the lake to be drained by October 29 and State officials stated the owner must present a final breach plan by November 4.
Source: <http://abc11.com/news/state-orders-woodlake-dam-owner-to-breach-it-and-drain/1572915/>

20. *October 25, Clarksburg Exponent-Telegram* – (West Virginia) **Two Lick Dam removal has begun.** The U.S. Fish and Wildlife Service began removing the Two Lick Dam in Clarksburg, West Virginia, October 25 to allow more than 30 miles of the West Fork River to flow freely, restore the snuffbox mussel and other federally listed species, and reduce the hydraulic roller effect that pushes people underwater. Officials expect the project to be completed in approximately 3 weeks.
Source: http://www.theet.com/news/local/two-lick-dam-removal-has-begun/article_b847e31b-d5ee-59eb-bea6-599980ccb62f.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.