



Daily Open Source Infrastructure Report 31 March 2016

Top Stories

- A clogged utility line in Woodland Park caused approximately 660,000 gallons of raw sewage to spill into Fountain Creek March 28, prompting Colorado Springs Utilities to open overflow pits to separate sewage. – *KOAA 5 Pueblo* (See item [14](#))
- Michigan authorities announced March 29 that at least 13 former and current principals in the Detroit Public Schools system were charged in a conspiracy scheme involving over \$900,000 in kickbacks and bribes in exchange for doing business worth \$2.7 million with Allstate Sales. – *NBC News* (See item [19](#))
- A security researcher discovered that hundreds of thousands of Internet of Things (IoT) printers were susceptible to attacks after finding that many IoT printers did not require authentication when connecting to the device. – *SecurityWeek* (See item [25](#))
- Two separate building fires March 29 caused a total of about \$600,000 in damages, prompted the closure of surrounding roads, and the evacuation of nearby areas in Salt Lake City. – *KSL 5 Salt Lake City* (See item [29](#))

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. *March 30, WTOP 103.5 FM Washington, D.C.* – (Virginia) **Power restored to thousands after Va. outage.** Dominion Power crews restored service March 30 to more than 23,000 customers in Loudoun County, Virginia, who lost power March 29 due to a reported problem with an underground cable.

Source: <http://wtop.com/loudoun-county/2016/03/power-outage-in-va-leaves-more-than-23000-without-power/>

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *March 30, WKBW 7 Buffalo* – (New York) **Faulty bolts raise concerns about Indian Point Nuclear Plant.** The New York governor reported March 29 that a recent inspection at the Indian Point Energy Center in Buchanan revealed that the nuclear plant's Unit 2 reactor had faulty bolts. There were no immediate threats to the public and officials stated the State will continue to investigate the plant's safety.

Source: <http://www.wkbw.com/news/state-news/faulty-bolts-raise-concerns-about-indian-point-nuclear-plant>

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *March 29, WCBS 2 New York City* – (New York) **Police: 2 men wanted in ATM skimming device incidents in Brooklyn, Queens.** Officials from the New York City Police Department and the FBI are searching March 29 for two men suspected of installing and removing ATM skimming devices at five different TD Bank locations in Brooklyn and Queens, New York, from September 2015 – November 2015.

Source: <http://newyork.cbslocal.com/2016/03/29/brooklyn-queens-atm-skimming/>

4. *March 29, Softpedia* – (International) **Repeated DDoS attacks force Coinkite Bitcoin wallet to close down web service.** One of the first Web-based bitcoin wallet services, Coinkite reported March 28 that it will be closing down its Web-based wallet service with the intention of solely developing its hardware products after their services received constant denial-of-service (DDoS) attacks for the past three years. The company warned users of potential phishing scams that will trick users into revealing their account credentials or tricking users into sending bitcoins to the wrong account.

Source: <http://news.softpedia.com/news/repeated-ddos-attacks-force-coinkit-bitcoin-wallet-to-close-down-web-service-502335.shtml>

5. *March 28, Middletown Times Herald-Record* – (New York) **Montgomery man pleads guilty in \$2.5 million fraud case.** Two Pennsylvania men and a New York resident pleaded guilty March 28 to Federal charges alleging that the trio defrauded banks from 2007 – 2015 by lying about their income in order to secure over \$2.5 million in fraudulent loans and lines of credit from banks and credit unions, then defaulting on the loans. Officials from the U.S. Attorney’s Office for the Southern District of New York stated that the trio used the loans to pay off credit card purchases, business expenses, and other loans to conceal the fraud.

Source: <http://www.recordonline.com/article/20160328/NEWS/160329452>

6. *March 28, U.S. Department of Justice* – (National) **Connecticut insurance salesman convicted of tax fraud.** The U.S. Department of Justice Tax Division announced March 28 that a Connecticut-based insurance salesman was found guilty of tax fraud after he attempted to obstruct the U.S. Internal Revenue Service (IRS) by filing 3 false tax returns for 2007, including a fraudulent request for a \$14 million refund, sending false and threatening correspondence to the IRS to defeat its assessment, collection, and investigative efforts, and by submitting threatening correspondence to those insurance companies that cooperated with IRS activities. Officials stated the salesman also established nominee entities to divert his insurance commissions in order to conceal assets and prevent the IRS from collecting on his tax liabilities.

Source: <https://www.justice.gov/opa/pr/connecticut-insurance-salesman-convicted-tax-fraud>

Transportation Systems Sector

7. *March 30, WIAT 42 Birmingham* – (Alabama) **I-20/59 westbound in Tuscaloosa shutdown after 2 vehicle accident involving 18-wheeler.** Westbound lanes of Interstate 20/59 in Tuscaloosa were shut down for several hours March 30 following a collision between a vehicle and a semi-truck that left two people injured when the driver of the vehicle fell asleep at the wheel and collided with the semi-truck.
Source: <http://wiat.com/2016/03/30/i20-westbound-shut-down-due-to-accident/>
8. *March 29, WFLA 8 Tampa* – (Florida) **Teen charged with leaving scene of fiery crash that killed truck driver.** One southbound lane of Interstate 75 in Sarasota reopened about 5 hours following a March 29 crash between a semi-truck transporting gasoline and another vehicle near Fruitville Road. The driver of the vehicle was apprehended by police several hours after fleeing the scene of the accident.
Source: <http://wfla.com/2016/03/29/fatal-tanker-fire-closes-i-75-in-sarasota/>
9. *March 29, Gallatin News Examiner* – (Tennessee) **Portland crash causes hazmat spill, closes Dobbins Pike.** Dobbins Pike in Portland, Tennessee, was closed for more than 6 hours March 29 while HAZMAT crews worked to clean up 11,000 pounds of fertilizer and 75 gallons of diesel fuel that spilled onto the roadway following a head-on collision between a vehicle and a farm truck.

Source: <http://www.tennessean.com/story/news/local/sumner/2016/03/29/sumner-emergency-crews-scene-two-car-crash/82384342/>

Food and Agriculture Sector

10. *March 29, U.S. Environmental Protection Agency* – (Washington) **EPA settles with Oregon Ice Cream Company over chemical safety violations.** The U.S. Environmental Protection Agency announced March 29 that the Oregon Ice Cream Company agreed to upgrade its refrigeration equipment to prevent toxic anhydrous ammonia releases, install leak detection systems, and improve overall safety and maintenance procedures to better prevent, detect, and safely respond to an accidental ammonia leak, among other safety improvements, after a 2011 inspection at the Eugene, Oregon facility revealed that the company violated the Federal Clean Air Act’s Risk Management Plan. As part of the settlement, Oregon Ice Cream Company has agreed to pay \$55,000 in penalties for its violations of Federal safety rules designed to prevent chemical emergencies.

Source:

<https://yosemite.epa.gov/opa/admpress.nsf/0/B2F46A996E54F0BF85257F85005600DD>

11. *March 29, U.S. Department of Labor* – (New York) **OSHA says food Rob Salamida Co. employee’s serious injuries due to fumes in 3,000-gallon vinegar tank ‘should never have happened’.** The Occupational Safety and Health Administration cited New York-based Rob Salamida Co. Inc., with 1 willful and 11 serious safety violations March 24 after a September 2015 incident hospitalized an employee and prompting an investigation at the Syracuse facility, which revealed that the company failed to provide safeguards to protect workers in confined spaces, failed to identify confined space hazards inside tanks, and failed to provide air monitoring, ventilation, and rescue equipment for employees in confined spaces, among other violations. Proposed penalties total \$79,600.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=30615

12. *March 29, U.S. Department of Labor* – (New Jersey) **US Labor Department settlement: Anheuser-Busch of New Jersey agrees to enhance safety for workers at its Jersey City, Bronx distributorships.** The Occupational Safety and Health Administration announced March 29 that it reached a settlement with Anheuser-Busch Sales of New Jersey LLC January 11 that requires the company to implement and maintain enhanced safety measures at its distributorships by conducting comprehensive safety and health self-audits, establishing safety and health committees comprised of management, employees, and unions, and ensuring adequate training, among other requirements. As part of the settlement, Anheuser-Busch has corrected the cited hazards at its Jersey City facility and paid a \$150,000 fine.

Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=30612

13. *March 29, Washington Post* – (Virginia) **Warehouse rack falls and kills a worker at Manassas food facility.** A rack system storing food products at Reinhart Foodservices warehouse in Manassas, Virginia, collapsed March 29, killing one employee and injuring seven others. Authorities from the Prince William County Fire Department are investigating the cause of the collapse.
Source: https://www.washingtonpost.com/local/public-safety/large-warehouse-rack-falls-and-injures-workers-at-manassas-food-facility/2016/03/29/aacec2e4-f5f2-11e5-8b23-538270a1ca31_story.html?hpid=hp_rhp-moreheds_pwrackfall610p%3Ahomepage%2Fstory

Water and Wastewater Systems Sector

14. *March 29, KOAA 5 Pueblo* – (Colorado) **More than 600,000 gallons of sewage spill into Fountain Creek.** A clogged utility line in Woodland Park caused approximately 660,000 gallons of raw sewage to spill into Fountain Creek March 28, prompting Colorado Springs Utilities to open overflow pits to separate any sewage that made it through. The raw sewage dissipated into the soil of the dried creek and health officials posted signs warning residents of the spill.
Source: <http://www.koaa.com/story/31594658/more-than-600000-gallons-of-sewage-spills-into-fountain-creek>

Healthcare and Public Health Sector

15. *March 30, SecurityWeek* – (International) **1,400 flaws found in outdated CareFusion Medical Systems.** CareFusion urged customers March 30 to upgrade its legacy systems to the latest version or follow a series of recommendations provided by the vendor to protect against potential attacks after two researchers discovered that legacy versions of Pyxis SupplyStation, which exist in seven different third-party software packages used by the CareFusion product, contain 1,418 vulnerabilities. Experts asserted that vulnerabilities pose little to no risk to patient safety as the system is designed to maintain critical functionality and provide access to medical supplies even if it is rendered inoperable.
Source: <http://www.securityweek.com/1400-flaws-found-outdated-carefusion-medical-systems>
16. *March 29, WEWS 5 Cleveland* – (Ohio) **Eight indicted for stealing more than \$750,000 from MetroHealth Medical Center.** Eight individuals were indicted for allegedly stealing over \$750,000 in property or services from MetroHealth Medical Center in Cleveland from October 2014 to February 2015 by distributing stolen outgoing hospital checks to people outside of Ohio who created bank accounts in the names of intended recipients in order to steal the money. The medical center stated that none of the individuals charged were ever employed by the company.
Source: <http://www.newsnet5.com/news/local-news/cleveland-metro/eight-indicted-for-stealing-more-than-750000-from-metrohealth-medical-center>

Government Facilities Sector

17. *March 30, Grand Rapids Press* – (Michigan) **Military training exercise to bring 1,000 soldiers to northern Michigan.** The National Guard of the United States will lead the Arctic Eagle exercise in Michigan from April 1 – April 14, an exercise which helps train soldiers to better respond to security issues in the Arctic. The exercise will include about 1,000 soldiers from the U.S. Army, U.S. Marine Corps, U.S. Coast Guard, and members of the Danish Army.
Source: http://www.mlive.com/news/grand-rapids/index.ssf/2016/03/national_guard_training_exerci.html
18. *March 30, WJLA 7 Washington, D.C.* – (Washington, D.C.) **Washington Monument opens Wednesday after elevator repairs.** The Washington Monument in Washington, D.C., will reopen March 30 following repairs after the Monument was closed March 29 due to a malfunctioning elevator.
Source: <http://wjla.com/news/local/washington-monument-scheduled-to-open-wednesday-after-elevator-repairs>
19. *March 29, NBC News* – (Michigan) **Feds charge 13 Detroit Public School principals in \$900K kickback scheme.** Michigan authorities announced March 29 that at least 13 former and current principals in the Detroit Public Schools system were charged in a conspiracy scheme involving over \$900,000 in kickbacks and bribes in exchange for doing business worth \$2.7 million with Allstate Sales, a vendor that provides school supplies.
Source: <http://www.nbcnews.com/news/us-news/feds-charge-13-detroit-public-school-principals-900k-kickback-scheme-n547341>
20. *March 29, SecurityWeek* – (National) **Marine Corps activates cyber warfare group.** The U.S. Marine Corps activated a new Cyberspace Warfare Group (MCCYWG) in Fort Meade, Maryland, March 25 which will help train and equip Marine Cyberspace mission teams to perform defensive and offensive cyber operations in support of the U.S. Cyber Command and U.S. Marine Corps Forces Cyberspace Command. The unit is active and will be fully operational in fiscal year 2017.
Source: <http://www.securityweek.com/marine-corps-activates-cyber-warfare-group>
21. *March 29, KCRA 3 Sacramento* – (California) **Measles case shuts down Nevada City charter school.** Yuba River Charter School in Nevada City was closed March 29 due to a confirmed case of measles in an unvaccinated child who traveled overseas. The school is scheduled to reopen March 30 to students who have been vaccinated, while students who have not been vaccinated will be required to stay home for an additional 3 weeks.
Source: <http://www.kcra.com/news/local-news/news-sierra/measles-case-shuts-down-nevada-city-charter-school/38745152>
22. *March 29, KTVT 11 Fort Worth* – (Texas) **Middle School closed Wednesday due to major electrical outage.** A power outage prompted the closure of Brewer Middle School in White Settlement March 30.

Source: <http://dfw.cbslocal.com/2016/03/29/middle-school-closed-wednesday-due-to-major-electrical-outage/>

Emergency Services Sector

23. *March 30, Buffalo News* – (New York) **Erie County 911 restored; backup system also failed.** Erie County’s 9-1-1 system was restored after a power failure forced the system to shut down for approximately 4 hours March 30. Calls were rerouted while crews restored power.

Source: <http://www.buffalonews.com/city-region/erie-county/erie-county-911-is-back-up-was-down-for-four-hours-20160330>

Information Technology Sector

24. *March 29, SecurityWeek* – (International) **“Vaccine” available for CTB-Locker, Locky, TeslaCrypt.** French cybersecurity company, Lexsi released a “vaccine” that can improve users’ computer defenses against ransomware including CTB-Locker, Locky, and TeslaCrypt and stated that users can create a specific mutex or registry key, or change the simple system parameter as long as the modification does not pose an inconvenience to other users.

Source: <http://www.securityweek.com/vaccine-available-ctb-locker-locky-teslacrypt>

25. *March 29, SecurityWeek* – (International) **Thousands of printers “hacked” to spew anti-semitic flyers.** A security researcher discovered that hundreds of thousands of Internet of Things (IoT) printers were susceptible to attacks after finding that many IoT printers did not require authentication when connecting to the device. The researcher found the vulnerability when using Masscan, a mass Internet Protocol (IP) scanner that collected all vulnerable printers in its vicinity.

Source: <http://www.securityweek.com/thousands-printers-hacked-spew-anti-semitic-flyers>

26. *March 29, Softpedia* – (International) **vBulletin servers hacked, admins force password reset for all users.** A company official for vBulletin.org and vBulletin.com reported that its Web domains went offline from March 24 – March 25 for a non-scheduled maintenance outage and forced its users to reset their passwords after hackers accessed the company’s vBulletin Germany (VGB) servers that carry user information. The exploit was allegedly reported to have used the content management system (CMS) used to run the company’s VGB’s presentation site.

Source: <http://news.softpedia.com/news/vbulletin-servers-hacked-admins-force-password-reset-for-all-users-502331.shtml>

For additional stories, see items [4](#), [20](#), and [28](#)

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

27. *March 30, WPIX 11 New York City* – (New York) **Massive Bushwick fire injures 11, displaces dozens of residents.** A March 29 fire in a Brooklyn residential building which housed several apartments, a church, and a karate school left at least 40 residents displaced, evacuated a total of 50 people, and injured 11 others. The incident prompted more than 200 firefighters to remain on site for over 3 hours containing the blaze.
Source: <http://pix11.com/2016/03/29/firefighters-battling-3-alarm-fire-in-bushwick/>
28. *March 29, Softpedia* – (International) **Magento stores targeted by new KimcilWare ransomware.** Security researchers from MalwareHunterTeam discovered a new ransomware dubbed KimcilWare was targeting Magento online stores and Web servers by encrypting users' Magento store files and adding the ".kimcilware" extension to each file, thus making the store inoperable. Researchers reported the ransomware was in its early stages of activity and were unsure about its mode of operation.
Source: <http://news.softpedia.com/news/magento-stores-targeted-by-new-kimcilware-ransomware-502328.shtml>
29. *March 29, KSL 5 Salt Lake City* – (Utah) **2 Salt Lake fires cause up to \$600K in damage.** Salt Lake City officials reported March 29 that 2 separate large building fires caused a total of about \$600,000 in damages, prompted the closure of surrounding roads, and the evacuation of nearby areas after one of the blazes allegedly began from an overheated fluorescent light ballast. Officials stated another fire began in a Salt Lake City warehouse March 28 after a fire used to keep people warm ignited propane bottles inside the facility.
Source: <https://www.ksl.com/?sid=39096233&nid=960&title=2-salt-lake-fires-cause-up-to-600k-in-damage>
30. *March 28, Wood County Sentinel-Tribune* – (Ohio) **Church, homes evacuated in BG gas main break.** The St. Aloysius Catholic Church and approximately a dozen nearby homes in Bowling Green, Ohio, were evacuated for an indeterminate amount of time March 28 after a contractor working on a water line project accidentally severed a six-inch gas line. Officials were unsure when repairs would be completed and no injuries were reported.
Source: <http://www.sent-trib.com/news/church-homes-evacuated-in-bg-gas-main->

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.