



Daily Open Source Infrastructure Report 23 December 2015

Top Stories

- An intense windstorm traveling across the Portland area December 21 caused power outages to approximately 30,000 people in several counties and closed railways and highways due to fallen trees and overturned vehicles. – *Portland Tribune* (See item [3](#))
- Carrier Corporation issued a recall December 22 for 285,000 of its Packaged Terminal Air Conditioners and Heat Pumps sold at HVAC dealers and factory-direct sales due to a potential fire hazard. – *U.S. Consumer Product Safety Commission* (See item [6](#))
- Ford Motor Company issued 3 safety recalls and 1 safety compliance recall December 22 for 317,677 of its various vehicles due to lighting control module issues, air brake chamber issues, and rear axle shaft issues, among other issues. – *Detroit News* (See item [8](#))
- Trend Micro researchers reported December 21 that cybercriminals behind Operation Black Atlas are using a variety of pen testing tools to exploit vulnerable systems within the healthcare and commercial sector to spread a variety of malware such as BlackPoS. – *SecurityWeek* (See item [13](#))

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. *December 22, Easton Express-Times* – (Pennsylvania) **Lehigh Valley biofuel entrepreneurs charged in \$50M federal scam.** The owners of Greenworks Holdings LLC and one predecessor were charged December 21 for their involvement in an alleged green energy scam in which they tricked the Federal government out of approximately \$50 million in payments, subsidies, and other benefits paid out for purportedly turning cooking oil into biofuel.
Source: http://www.lehighvalleylive.com/news/index.ssf/2015/12/lehigh_valley_biofuel_entrep_re.html
2. *December 21, Associated Press* – (National) **Duke Energy battles off steady cyberattacks.** A spokesperson for Duke Energy Corp., announced December 21 that the company is on alert for cyberattacks and that its computer systems are under constant attack. The utility is working with U.S. intelligence agencies to help prevent and mitigate any potential threats against its systems.
Source: <http://www.newsobserver.com/news/business/article50946705.html>
3. *December 21, Portland Tribune* – (Oregon) **Monday windstorm knocks out power, shuts down highway.** An intense windstorm traveling across the Portland area December 21 caused power outages to approximately 30,000 people in several counties and closed railways and highways due to fallen trees and overturned vehicles.
Source: <http://www.pamplinmedia.com/pt/9-news/286192-163074-monday-windstorm-knocks-out-power-shuts-down-highway>

For another story, see item [13](#)

Chemical Industry Sector

4. *December 21, WCMH 4 Columbus* – (Ohio) **Crews clear scene after explosion at Newark manufacturing plant.** A December 21 fire at Arboris LCC, a manufacturing facility for plant sterols, injured 5 people and prompted 20 fire trucks to remain on site for over 3 hours after the fire began when a pressurized tank containing hexane and ethanol exploded inside its Newark facility. The exact cause of the incident was not disclosed.
Source: <http://nbc4i.com/2015/12/21/fire-reported-at-newark-industrial-plant/>

Nuclear Reactors, Materials, and Waste Sector

5. *December 22, Associated Press* – (Minnesota) **NRC says Xcel Energy agrees to corrective measures at plant.** The U.S. Nuclear Regulatory Commission (NRC) reported that Xcel Energy Inc., agreed to implement corrective actions to address improper testing of welds on six spent fuel canisters at the company's Monticello nuclear plant December 21 after two NRC inspectors falsely recorded testing examinations to cover the plant's failure to implement effective quality controls, putting the plant in violation of the agency requirements. The NRC found no immediate

safety concerns with the canisters.

Source: http://lacrossetribune.com/news/state-and-regional/mn/nrc-says-xcel-energy-agrees-to-corrective-measures-at-plant/article_fba69a2a-d130-5ce1-a95b-9ae0c1f5b886.html

Critical Manufacturing Sector

6. *December 22, U.S. Consumer Product Safety Commission* – (National) **Carrier recalls to repair packaged terminal air conditioners, heat pumps including previously recalled units due to fire hazard.** Carrier Corporation issued a nationwide recall December 22 for 285,000 of its Carrier, Bryant and Fast branded Packaged Terminal Air Conditioners and Heat Pumps sold at HVAC dealers and factory-direct sales due to a potential fire hazard following 47 reported incidents of the units overheating and 1 incident of consumer injury.
Source: <http://www.cpsc.gov/en/Recalls/2016/Carrier-Recalls-to-Repair-Packaged-Terminal-Air-Conditioners-Heat-Pumps-Previously-Recalled-Units/>
7. *December 22, U.S. Consumer Product Safety Commission* – (National) **Breville recalls pressure cookers due to risk of burns.** Breville USA Inc., issued a recall December 22 for around 35,600 of its 6-quart capacity Fast Slow Cookers due to a risk of burns to the user after five customer reports revealed that an unexpected release of built-up pressure was caused by incorrectly inserting the sealing gasket on the lid. The product was sold to several retail stores nationwide and through Internet sales.
Source: <http://www.cpsc.gov/en/Recalls/2016/Breville-Recalls-Pressure-Cookers/>
8. *December 22, Detroit News* – (International) **Ford issues four recalls for about 317K vehicles.** Ford Motor Company issued 3 safety recalls and 1 safety compliance recall December 22 for 313,000 of its 2003 – 2005 model year Crown Victoria and Mercury Grand Marquis vehicles for lighting control issues; 177 of its 2016 model year F-650 and F-750 trucks for air brake chamber issues; 1,300 of its 2015 model year Transit dual-rear-wheel vehicles for rear axle shaft issues; and 3,200 of its 2015 model year F-150 SuperCrew vehicles for front seat belt retractor and pretension assembly issues. Officials stated that 11 reports of accidents and 1 report of minor injury were linked to the Crown Victoria and Mercury Grand Marquis vehicles and no accidents have been reported in relation to the other vehicles.
Source: <http://www.detroitnews.com/story/business/autos/ford/2015/12/22/ford-issues-four-recalls/77741848/>
9. *December 21, WMUR 9 Manchester* – (New Hampshire) **Ball bearing company to pay \$150K penalty after explosion.** New Hampshire Ball Bearings agreed to pay a \$150,000 penalty to the New Hampshire Department of Environmental Services December 21 following a factory explosion caused by a chemical reaction that built up pressure inside a steel drum at its Peterborough plant which injured 15 people February 2014.
Source: <http://www.wmur.com/news/ball-bearing-company-to-pay-150k-penalty-after-explosion/37069692>

10. *December 21, U.S. Department of Labor* – (Pennsylvania) **Milton, Pennsylvania, manufacturer cited for workplace safety and health hazards after employee sustains 2nd- and 3rd- degree burns.** The U.S. Occupational Safety & Health Administration cited railcar parts manufacturer and fabricator, ACF Industries LLC for one willful and three serious violations December 8 after an inspection at its Milton facilities revealed an untrained employee suffered second- and third- degree burns while operating a blasting machine without proper protection. Proposed penalties total \$87,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=29295

For another story, see item [13](#)

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

11. *December 21, Easton Express-Times* – (Pennsylvania) **Ex-Allentown finance director charged with role in pay-to-play scheme.** The U.S. Attorney’s Office announced December 21 that Allentown’s former finance director was charged with conspiracy to commit mail and wire fraud following a pay-to-play scheme in which the director falsified public records in order to help award a contract to a campaign donor who supported the city Mayor.
Source: http://www.lehighvalleylive.com/allentown/index.ssf/2015/12/ex-allentown_finance_director.html
12. *December 21, New York Post-Star* – (New York) **Queensbury man pleads guilty in \$1.2 million financial scheme.** A former financial adviser pleaded guilty December 21 in Albany County Court to counts of grand larceny, scheme to defraud, money laundering, and violating state business law for his involvement in a Ponzi scheme in which he stole more than \$1.26 million from 10 clients and paid some clients by taking the funds from others.
Source: http://poststar.com/news/blotter/queensbury-man-pleads-guilty-in-million-financial-scheme/article_50809834-29e4-53f3-ab7b-dc1f92d5f56f.html
13. *December 21, SecurityWeek* – (National) **Operation Black Atlas continues to compromise PoS systems.** Trend Micro researchers announced December 21 that cybercriminals behind Operation Black Atlas are using a variety of pen testing tools to exploit vulnerable systems within the healthcare and commercial sector to spread a variety of malware such as BlackPoS; steal user credentials to Web sites that contain sensitive information; abuse the Windows Background Intelligent Transfer Service (BITS) or bitsadmin.exe; and build a replica of the Gorynych / Diamond Fox botnet malware and repurposed it to specifically look for the output file of the BlackPoS malware, which includes harvested credit card data, among other malicious actions.

Source: <http://www.securityweek.com/operation-black-atlas-continues-compromise-pos-systems>

Transportation Systems Sector

14. *December 21, WITN 7 Washington* – (North Carolina) **Highway 17 reopens after 18-wheeler accident.** Highway 17 in Bertie County was closed for several hours December 21 while officials worked to clear the wreckage and gas spill from an overturned semi-truck.
Source: <http://www.witn.com/home/headlines/18-wheeler-carrying-LP-gas-overturns-officials-warn-drivers-to-avoid-area-363110721.html>
15. *December 21, Sidney Sun-Telegraph* – (Nebraska) **UP train collides with semi, derails.** A Union Pacific train traveling from Oregon to Chicago collided with a semi-truck in Sidney December 21 causing a shutdown of U.S. Highway 30 for several hours. Officials are investigating what caused the semi-truck to stop at the railroad crossing.
Source: <http://www.suntelegraph.com/story/2015/12/21/community/up-train-collides-with-semi-derails/8763.html>
16. *December 21, KDVR 31 Denver* – (Colorado) **2 killed in double fatal crash in Douglas County, Highway 83 closed.** Highway 83 in Douglas County was closed for several hours December 21 while officials investigated a fatal 2-vehicle crash that killed 2 people.
Source: <http://kdvr.com/2015/12/21/2-killed-in-double-fatal-crash-in-douglas-county-highway-83-closed/>
17. *December 21, KOB 4 Albuquerque*– (New Mexico) **Overturned semi, hazmat situation closes NM 68 north of Velarde.** New Mexico State Road 68 in Taos reopened December 22 after being closed December 21 while HAZMAT crews worked to clear the wreckage and a fuel spill from an overturned semi-truck that spilled fuel and severely burned the highway.
Source: http://www.kob.com/article/stories/s3998193.shtml#.VnltH_krKUK

For another story, see item [3](#)

Food and Agriculture Sector

18. *December 22, USA Today* – (National) **Chipotle linked to a second E. coli outbreak.** The Centers for Disease Control and Prevention (CDC) announced December 21 that it is investigating a second E. coli outbreak after at least five people fell ill after consuming food from the Chipotle Mexican Grill restaurants in North Dakota, Kansas, and Oklahoma.
Source: <http://www.msn.com/en-us/news/us/chipotle-linked-to-a-second-e-coli-outbreak/ar-BBnNpwB?li=BBnbcA1>
19. *December 21, U.S. Food and Drug Administration* – (Washing; Florida) **The**

Swinomish Fish Company voluntarily recalls Native Catch Salmon Bacon because of a possible health risk. The Swinomish Fish Company issued a voluntary recall December 21 for its Traditional Native Catch Salmon Bacon and Peppered Native Catch Salmon Bacon products distributed to retailers in Washington and Florida after routine inspection discovered the products were under processed and may have been contaminated with Clostridium botulinum.

Source: <http://www.fda.gov/Safety/Recalls/ucm478558.htm>

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

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

See item [13](#)

Government Facilities Sector

20. *December 21, WBAL 11 Baltimore* – (Maryland) **36 people assessed after carbon monoxide leak in Kent County.** A carbon monoxide leak due to a malfunctioning heating system at the Department of Social Services building in Chestertown prompted 36 people to be treated on site December 21.

Source: <http://www.wbaltv.com/news/36-people-assessed-after-carbon-monoxide-leak-in-kent-county/37067700>

21. *December 20, CNN* – (Washington, D.C.) **Man arrested after jumping fence, entering Treasure building.** The U.S. Secret Service reported that a man was arrested and charged December 18 for unlawful entry after he allegedly jumped a fence and entered the U.S. Department of The Treasure building located next to the White House. A complete search of the exterior of the building and the White House grounds were conducted and officials deemed the area safe.

Source: <http://wqad.com/2015/12/20/man-arrested-after-jumping-fence-entering-treasury-building/>

Emergency Services Sector

22. *December 22, Delaware County Daily Times* – (Delaware) **Chief, 2 others charged in \$50,000 theft from Colwyn Fire Company.** Three former Colwyn Borough Volunteer Fire Company officials were charged with third-degree felony by unlawful taking, theft by deception, theft by failure to make required dispositions of funds, and receiving stolen property, as well as conspiracy counts for each charge December 21 after a 10-month investigation revealed that the trio stole money from the company and used the funds for personal gain instead of paying the fire department's bills for numerous months.

Source: <http://www.delcotimes.com/article/DC/20151221/NEWS/151229951>

Information Technology Sector

23. *December 22, SecurityWeek* – (International) **Oracle settles FTC charges over Java security updates.** The U.S. Federal Trade Commission reported that the computer technology company, Oracle Corporation agreed to settle charges that the company deceived its customers by failing to notify its users that the Java Standard Edition (SE) updates only removed the most recent version of SE and not previously vulnerable versions, which exposed users to potential attacks. Oracle will be required to warn users during a SE update if older software version are present, to inform users about risks, and to present options to remove the vulnerable applications, among other requirements.
Source: <http://www.securityweek.com/oracle-settles-ftc-charges-over-java-security-updates>
24. *December 21, SecurityWeek* – (International) **TeslaCrypt delivered via recently patched flash exploit.** Researchers from Malwarebytes reported that the previously patched Flash Player heap buffer overflow vulnerability (CVE-2015-8446), which was added to the Angler exploit kit, was exploited by attackers to deliver a new variant of the TeslaCrypt ransomware that encrypts files and renames them with a .vvv extension. Once the files are encrypted, victims are instructed to pay the attackers monetary funds to receive the private key needed to decrypt the files.
Source: <http://www.securityweek.com/teslacrypt-delivered-recently-patched-flash-exploit>
25. *December 21, Softpedia* – (International) **Gomasom ransomware decrypted, get your files back for free.** A security researcher at Emsisoft created a tool for decrypting files, previously encrypted by the Gomasom ransomware that allows affected users to take the encrypted files and obtain the decryption key without paying the ransomware. The tool allows victims to use files in both its ransomware-encrypted and original version, or a ransomware-encrypted PNG file to retrieve the lost data.
Source: <http://news.softpedia.com/news/gomasom-ransomware-decrypted-get-your-files-back-for-free-497945.shtml>

For another story, see item [13](#)

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

26. *December 22, Annapolis Capital Gazette* – (Maryland) **Two-alarm fire damages Crofton condos.** A 2-alarm fire at a Crofton condominium building caused \$100,000 in damages and displaced 1 resident December 22 after the fire began in 1 apartment unit and spread to 2 adjacent units. The cause of the fire remains under investigation, but preliminary investigations reveal the incident was accidental.
Source: http://www.capitalgazette.com/news/for_the_record/ph-ac-cn-crofton-condo-fire-1223-20151222-story.html
27. *December 21, WKMG 6 Orlando* – (Florida) **Walmart in Apopka cleared after bomb threat, police say.** A Walmart in Apopka, Florida was evacuated for approximately 3 hours December 21 after the store received a phone-in bomb threat. Officials searched the building and found no explosive devices.
Source: <http://www.clickorlando.com/news/threat-evacuates-walmart-in-apopka>
28. *December 20, Portland Tribune* – (Oregon) **Landslides prompt Oregon City apartment evacuation.** Oregon City officials issued an evacuation notice requiring 10 families at the Berry Hill Apartments to evacuate their units and issued a voluntary evacuation notice for families in 60 apartment units at the Forest Edge Apartment Complex December 21 following reports of landslide hazards. The American Red Cross is assisting displaced residents by opening an emergency shelter.
Source: <http://portlandtribune.com/pt/9-news/286172-163039-landslides-prompt-oregon-city-apartment-evacuation>

For another story, see item [13](#)

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.