



Daily Open Source Infrastructure Report 30 December 2015

Top Stories

- Fiat Chrysler Automobiles issued 2 recalls December 27 for more than 412,938 of its Jeep Grand Cherokee, Dodge Durangos, Compass, and Patriot vehicles distributed in the U.S. due to a vanity mirror wiring and clamp issue that can cause a fire. – *Autoblog* (See item [3](#))
- Two former employees of Jaycal Tax Service in Phenix City, Alabama, pleaded guilty December 28 for their roles in an identity theft scheme that stole over 1,000 identities between 2007 and 2012. – *Montgomery Advertiser* (See item [5](#))
- Adobe released out-of-band security updates that addressed several vulnerabilities in its Flash Player products which affects all platforms and can allow an attacker to take control of an infected system through a spear phishing campaign. – *SecurityWeek* (See item [20](#))
- Researchers from Palo Alto Networks discovered that a total of 11,149 computers were infected by new malware dubbed ProxyBack, which targets personal computers and educational institutes in Europe. – *Softpedia* (See item [21](#))

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 29, WMAQ 5 Chicago; Chicago Sun-Times* – (Illinois) **Nearly 90,000 Chicago area residents lose power in Monday's storm.** Commonwealth Edison crews worked to restore power to approximately 12,000 customers that remained without service December 29 following a wintry mix of sleet, rain, and snow that knocked out power to nearly 90,000 customers December 28.
Source: <http://www.nbcchicago.com/news/local/Nearly-90000-Chicago-Area-Residents-Lose-Power-in-Storm-363714011.html>
2. *December 29, Associated Press* – (Indiana) **Utility estimates 2 more days to fix thousands of power outages scattered in northern Indiana.** Utility crews worked December 29 to restore power to at least 25,000 homes and businesses in northern Indiana that remained without service following severe weather December 28.
Source:
<http://www.therepublic.com/view/story/5eeced287f4d4275b0f54e3337b1f0e3/IN--Severe-Weather-Indiana>

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *December 27, Autoblog* – (International) **FCA recalls 570,000 SUVs from Jeep and Dodge over fire woes.** Fiat Chrysler Automobiles (FCA) issued two recalls December 27 for 352,831 of its model year 2011 – 2012 Jeep Grand Cherokee vehicles and models built before 2012 Dodge Durango vehicles due to a vanity mirror wiring issue, as well as 60,107 of its model year 2015 Jeep Compass and Patriot vehicles distributed in the U.S. due to an out-of-position clamp that could lead to a leak in the power steering fluid line and pose a fire hazard or loss of power-steering.
Source: <http://www.autoblog.com/2015/12/27/jeep-grand-cherokee-dodge-durango-recall/>

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *December 29, Quincy Patriot Ledger* – (Massachusetts) **Quincy Credit Union works to replace debit cards, stolen money.** Quincy Credit Union reported that at least 675 of its customers' accounts were compromised the weekend of December 26 after

officials found hackers had installed an ATM skimming device to the company's machines. Officials believe hackers installed the malicious devices early December and later created duplicate cards, which were used to withdraw cash at ATMs throughout New York City.

Source: <http://www.patriotledger.com/news/20151228/quincy-credit-union-works-to-replace-debit-cards-stolen-money>

5. *December 28, Montgomery Advertiser* – (Alabama) **2 plead guilty to ID theft, \$4 million in tax fraud.** Two former employees of Jaycal Tax Service in Phenix City pleaded guilty December 28 to aggravated identity theft and conspiring to defraud the government after the two obtained more than 1,000 stolen identities, filed over 1,200 false Federal tax returns, and claimed more than \$4 million in fraudulent returns between 2007 and 2012.

Source: <http://www.montgomeryadvertiser.com/story/news/crime/2015/12/28/2-plead-guilty-id-theft-claiming-4-million-false-returns/77970688/>

Transportation Systems Sector

6. *December 29, Associated Press* – (National) **Latest storm system dumps snow in Midwest, cancels scores of flights.** Officials reported December 29 that over 2,800 flights across the U.S. were cancelled while 4,800 were delayed December 28 due to a severe storm that moved through several States and led to about 4 dozen deaths. Highways were forced to close while counties in Missouri, Texas, and Mississippi announced disaster declarations.

Source: <http://www.foxnews.com/us/2015/12/29/latest-storm-system-dumps-snow-in-midwest-cancels-scores-flights.html>

7. *December 29, WTOP 103.5 FM Washington, D.C.* – (Maryland) **Glenmont Metro station reopens after smoke prompts evacuation.** Train service at the Glenmont Metro station in Silver Spring was halted for approximately 2 hours December 28 due to reports of a possible electrical fire that prompted the station's evacuation. Crews cleared the scene and an investigation into the discovery of smoke in the tunnel is ongoing.

Source: <http://wtop.com/sprawl-crawl/2015/12/glenmont-metro-station-reopens-fire-smoke-prompts-evacuation/>

8. *December 29, WFMZ 69 Allentown* – (Pennsylvania) **Easton-area man killed in Route 611 crash.** Route 611 in Northampton County was closed for several hours December 28 while police investigated the scene of a head-on collision that left one driver dead and a second driver injured.

Source: <http://www.wfmz.com/news/news-regional-lehighvalley/accident-closes-route-611-in-northampton-county/37164144>

9. *December 29, Associated Press* – (New York) **Police: 1 killed in 2-vehicle crash on I-90 outside Albany.** Several lanes of Interstate 90 in East Greenbush were closed for more than 9 hours December 29 while officials investigated the scene of a fatal 2-vehicle crash involving a FedEx semi-truck and another vehicle that left 1 driver dead.

Source: <http://www.sfgate.com/news/article/Crash-involving-truck-van-closes-I-90-lanes-6725332.php>

10. *December 28, KYTV 3 Springfield* – (Missouri) **Train derails in flood waters in Neosho.** Floodwater from Shoal Creek swept 30 containers from a stopped BNSF Railway train off its tracks in Neosho December 27, forcing the indefinite closure of the tracks until repairs are completed.

Source: http://www.ky3.com/news/local/21048998_37166228

Food and Agriculture Sector

11. *December 28, Associated Press* – (New York) **Whole Foods to pay \$500K to settle overcharging allegations.** Whole Foods Market Inc., agreed to pay \$500,000 to New York City's Department of Consumer Affairs to settle allegations that the company overcharged customers for pre-packaged foods December 28 after an investigation revealed 80 different types of pre-packaged food items had mislabeled weights. Whole Foods Market Inc., will also be required to conduct quarterly audits to ensure products are accurately weighed and labeled.

Source: <http://www.foxnews.com/us/2015/12/28/whole-foods-to-pay-500k-to-settle-overcharging-allegations.html>

12. *December 28, Fresno AgNet West Radio Network* – (California) **Asian citrus psyllid quarantine in Stanislaus County includes portion of Merced County.** Officials reported that Southern Stanislaus County and a portion of Merced County were under quarantine after the Asian citrus psyllid (ACP), which can carry fatal diseases to citrus plants, were found in the City of Turlock December 28. The quarantine zone includes up to 21 counties in California and prohibits the sale or movement of citrus plants and curry leaf trees and requires all fruits to be cleaned of leaves and stems prior to leaving the quarantine area.

Source: <http://agnetwest.com/2015/12/28/asian-citrus-psyllid/>

13. *December 28, U.S. Food and Drug Administration* – (New Jersey) **Uoriki Fresh, Inc. recalls "Octopus Salad" because of possible health risk.** Secaucus-based Uoriki Fresh, Inc., issued a voluntary recall December 28 for its Octopus Salad product packaged in eight-ounce plastic trays after routine testing revealed the presence of *Listeria monocytogenes*. The item was sold to one Wegmans Food Market store in Manalapan, New Jersey.

Source: <http://www.fda.gov/Safety/Recalls/ucm479172.htm>

For another story, see item [23](#)

Water and Wastewater Systems Sector

14. *December 29, St. Louis Metropolitan Sewer District* – (Missouri) **Fenton wastewater treatment plant shutdown.** The Metropolitan St. Louis Sewer District announced December 29 that the Fenton Wastewater Treatment Plant stopped operating December 28 due to heavy rainfall and the rising Meramec River which resulted in a water

overflow and a power outage. Officials urged the public to avoid contact with any flood water or sewage near the plant while sewage is being diverted to nearby rivers and streams.

Source: <http://www.stlmsd.com/blog/fenton-wastewater-treatment-plant-shutdown?hootPostID=9e1a52ac3f37cf28f04487c177f51da9>

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

15. *December 27, University of Connecticut, Daily Campus* – (Connecticut) **UConn website compromised, prompting users to download malicious program.** The University of Connecticut reported that its Web site was compromised December 27 prompting visitors to download a malicious program posing as Adobe Flash Player instead of allowing access to content on the university's site. Officials reported that it restored the Web site's Domain Name System (DNS) records, but warned that the problem continued to persist for some users.

Source: <http://dailycampus.com/stories/uconn-website-compromised-malicious-program>

For another story, see item [21](#)

Emergency Services Sector

16. *December 29, WPTV 5 West Palm Beach* – (Florida) **Two Boynton Beach fire stations closed over air quality.** The mayor of Boynton Beach announced December 29 that Fire Station 3 and Fire Station 1 will remain closed until air sampling tests are complete following the October and November closures of both stations due to air quality issues. All personnel were relocated to other buildings during testing and cleaning of the air ducts.

Source: <http://www.wptv.com/news/region-s-palm-beach-county/boynton-beach/2-boynton-beach-fire-stations-closed-over-mold-concerns>

17. *December 27, Washington County Observer-Reporter* – (Pennsylvania) **Sister accused of helping inmate escape Greene County jail.** Authorities arrested a Dilliner woman for allegedly helping her brother escape from the Greene County jail in Pennsylvania December 27. The jail was placed under lockdown through December 28 and the inmate remains at large.

Source: http://www.observer-reporter.com/20151227/sister_accused_of_helping_inmate_escape_greene_county_jail

Information Technology Sector

18. *December 29, Softpedia* – (International) **AVG forcibly installs vulnerable Chrome**

extension that exposes users' browsing history. A researcher from Google Project Zero discovered a serious vulnerability in the AVG Web TuneUp Chrome extension, which was forcibly installed when users downloaded the AVG Antivirus that allowed attackers to access users' cookies, browsing history, and other details by executing cross-site scripting (XSS) attacks and cross-domain requests. AVG Web TuneUp Version 4.2.5.169 patched the flaw and Google blocked AVG's inline installation of the extension.

Source: <http://news.softpedia.com/news/avg-forcibly-installs-vulnerable-chrome-extension-that-exposes-user-s-browsing-history-498187.shtml>

19. *December 28, SecurityWeek* – (International) **Android malware uses firewall rules to block security apps.** Researchers from Symantec discovered a new Microsoft Android malware, dubbed Android.Spywaller, that allows attackers to block mobile security applications, exfiltrate sensitive data from compromised mobile devices including personally identifying information (PII), and collect data belonging to specific third-party communication applications including BlackBerry Messenger, Oovoo, and Skype, among others, through a reverse payload attack that drops and runs the DroidWall firewall binary to create firewall rules and block the application's security using its own unique identifier (UID). The malware was seen targeting users in China via the Qihoo 360 application and researchers advised users to install security solutions to block mobile threats, update software regularly, and install applications from trusted sources.

Source: <http://www.securityweek.com/android-malware-uses-firewall-rules-block-security-apps>

20. *December 28, SecurityWeek* – (International) **Adobe issues emergency patch for flash zero-day under attack.** Adobe released out-of-band security updates that addressed several vulnerabilities in its Flash Player products including a type confusion vulnerability, an integer overflow vulnerability, a use-after-free vulnerability, and a memory corruption vulnerability that affects all platforms and can allow an attacker to take control of an affected system through a spear phishing campaign.

Source: <http://www.securityweek.com/adobe-issues-emergency-patch-flash-zero-day-under-attack>

21. *December 28, Softpedia* – (International) **ProxyBack malware turns infected computers into internet proxies.** Researchers from Palo Alto Networks discovered that a total of 11,149 computers were infected by the new malware, ProxyBack, which targets personal computers (PC) and educational institutes in Europe by altering infected devices into Internet proxies while illegally using them to transfer Internet traffic via an established connection with a malicious proxy server, where it receives instructions to route traffic to attackers' Web servers. Each affected device works as a bot inside a larger network to send commands and updated instructions via simple Hypertext Transfer Protocol (HTTP).

Source: <http://news.softpedia.com/news/proxyback-malware-turns-infected-computers-into-internet-proxies-498167.shtml>

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

22. *December 28, WABC 7 New York City* – (New York) **2 dead after fire burns through apartment building in Williamsburg.** A 5-alarm fire at a Williamsburg apartment building displaced 10 residents and killed 2 others December 28, prompting about 200 firefighters to remain on site for about 3 hours containing the incident. The cause of the fire is under investigation and officials believe the fire started on the first floor.
Source: <http://abc7ny.com/news/2-dead-after-fire-burns-through-apartment-building-in-williamsburg/1137720/>
23. *December 28, KHOU 11 Houston* – (Texas) **Pappas BBQ in Humble closed after 2-alarm fire overnight.** Officials reported that the Pappas BBQ in Humble, Texas, was closed indefinitely December 28 after a 2-alarm fire begin in the kitchen grill/smoking pit and spread to the roof. No injuries were reported and the Humble Fire Marshal is investigating the cause of the incident.
Source: <http://www.khou.com/story/news/local/neighborhood/2015/12/28/pappas-bbq-humble-closed-after-2-alarm-fire-overnight/77964176/>
24. *December 28, WBAY 2 Green Bay* – (Wisconsin) **Body and mysterious liquid found at Green Bay motel prompts evacuation.** Officials reported December 28 that the Economy Inn in Green Bay was evacuated while HAZMAT crews cleared the scene of a frothing and bubbling liquid substance found in a motel room, where a man was found dead. Officials reported the liquid did not pose any immediate danger.
Source: <http://wbay.com/2015/12/28/body-and-mysterious-liquid-found-at-green-bay-motel-prompts-evacuation/>

For additional stories, see items [2](#) and [6](#)

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.