



Daily Open Source Infrastructure Report 24 December 2015

Top Stories

- Boeing Company agreed to pay \$12 million December 22 to resolve several violations, including the company's failure in meeting a deadline for the submission of airplane service instructions. – *Associated Press* (See item [7](#))
- Federal authorities issued an alert December 22 to drug compounders claiming that drug shipments from China may be contaminated following two explosions at a Tianjin chemical warehouse in August. – *U.S. Food and Drug Administration* (See item [12](#))
- Sanrio Co., Ltd reported December 22 that it fixed a security vulnerability on an online fan Web site after the personal information of 3.3 million users were compromised. – *Associated Press* (See item [17](#))
- Police in Oregon are investigating December 22 after 2 men were found in possession of 470 Apple iPhones products worth \$292,000, as well as hundreds of fraudulent gift cards and receipts. – *Portland Oregonian* (See item [18](#))

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

See item [14](#)

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

1. *December 23, Waco Tribune-Herald* – (Texas) **Skimmers hit Extraco Banks credit, debit cards.** Texas-based Extraco Banks announced December 22 that at least 265 customers had their bank-issued credit and debit cards illegally accessed through skimming devices placed on ATM machines and/or merchant terminals. An investigation is ongoing and the bank has taken additional security steps, including lowering daily withdrawal and purchase amounts, as well as limiting the amount of fraud that could occur if a card is compromised.
Source: http://www.wacotrib.com/news/business/skimmers-hit-extraco-credit-debit-cards/article_515689d1-4a06-576d-a484-998c23724280.html
2. *December 23, Associated Press* – (Maryland; West Virginia) **Developer pleads guilty in \$5.7 million bank fraud scheme.** A developer pleaded guilty December 22 to charges connected to a scheme that fraudulently obtained \$5.7 million in real estate loans for properties in Maryland's Deep Creek Lake and West Virginia's Cheat Lake. Two other co-conspirators were previously convicted for their roles in the scheme.
Source: https://www.washingtonpost.com/local/developer-pleads-guilty-in-57-million-bank-fraud-scheme/2015/12/23/02bc562c-a979-11e5-b596-113f59ee069a_story.html
3. *December 23, CNBC* – (National) **Federal Reserve vulnerable to hackers: Inspector general.** A report released December 23 by the inspector general for the U.S. Federal Reserve System warned that there are several cybersecurity deficiencies in the Federal Reserve Board's Statistics and Reserves (STAR) system. The report included six recommendations for improvements to the system's security controls in areas including planning, security assessment and authorization, contingency planning, auditing, and information integrity, among other areas.

Source: <http://www.cnbc.com/2015/12/23/federal-reserve-vulnerable-to-hackers-inspector-general.html>

4. *December 23, WHAS 11 Louisville* – (Kentucky) **3 arrested in credit card ‘skimming’ operation.** Police arrested three individuals following the discovery of 86 prepaid debit cards that were re-coded with stolen credit card numbers in their vehicle during a traffic stop on Preston Highway in Louisville December 21.
Source: <http://www.whas11.com/story/news/crime/2015/12/22/3-arrested-credit-card-skimming-operation/77772768/>
5. *December 22, Reuters* – (National) **Morgan Stanley to pay U.S. SEC \$8.8 million in ‘parking’ scheme case.** The U.S. Securities and Exchange Commission announced December 22 that Morgan Stanley Investment Management Inc., will pay \$8.8 million to settle charges that one of its portfolio managers took part in pre-arranged trading or “parking” which included arranging sales of mortgage-backed securities at predetermined prices to a trader at the Societe Generale brokerage unit, SG Americas. The sales allowed the portfolio manager to buy back the positions at a small markup into other accounts that Morgan Stanley advised.
Source: <http://www.reuters.com/article/us-morganstanley-fine-idUSKBN0U520N20151222>

For another story, see item [18](#)

Transportation Systems Sector

6. *December 23, WRAL 5 Raleigh* – (North Carolina) **Truck carrying pigs crashes on I-40 West; crews work to clean up mess.** Police reported that 2 right lanes of Interstate 40 west in Raleigh were shut down for several hours December 22 while crews worked to clear the wreckage from a crash involving a semi-truck carrying 2,200 pigs that ran off the road and went down an embankment. Several pigs were killed in the accident.
Source: <http://www.wral.com/truck-carrying-pigs-crashes-on-i-40-blocking-2-lanes/15192062/>
7. *December 22, Associated Press* – (International) **Boeing fined \$12M for failing to quickly address fuel tank blast risk.** Boeing Company agreed to pay \$12 million in a settlement reached December 22 with the Federal Aviation Administration resolving several violations including the company’s failure in meeting a deadline for the submission of service instructions that would enable airlines to reduce the risk of fuel tank explosion on hundreds of plans. The settlement also resolves production quality control problems and failures to implement corrective actions, among other issues.
Source: <http://www.nbcnews.com/business/travel/boeing-fined-12m-failing-quickly-address-fuel-tank-blast-risk-n484551>
8. *December 22, WDAF 4 Kansas City* – (Missouri) **Concrete truck flips over on I-35, jamming southbound lanes for several hours.** Southbound lanes of Interstate 35 in Kansas City, Missouri, were closed for approximately 3 hours December 22 while crews worked to clear the wreckage from an overturned semi-truck that was carrying

cement. The driver sustained minor injuries and officials are investigating the incident.
Source: <http://fox4kc.com/2015/12/22/concrete-truck-flips-over-on-i-35-shuts-down-highway/>

Food and Agriculture Sector

9. *December 22, U.S. Food and Drug Administration* – (California) **Ocean Group, Inc. announces recall of Ocean Brand Masago Lake Smelt Roe for undeclared allergens.** Los-Angeles based-Ocean Group, Inc., issued a recall December 17 for all of its Masago Lake Smelt Roe products packaged in 6-ounce clear cups due to misbranding and undeclared wheat and soy allergens. The company will send recall notices to all of its direct customers.
Source: <http://www.fda.gov/Safety/Recalls/ucm478780.htm>
10. *December 22, U.S. Food and Drug Administration* – (National) **Bee Extremely Amazed LLC issues voluntary nationwide recall of various products distributed for weight loss due to undeclared drug ingredients.** Bee Extremely Amazed LLC issued a voluntary recall December 22 for several of its weight loss products due to misbranding and undeclared drug ingredients including sibutramine and/or phenolphthalein, which are withdrawn and unapproved for use in U.S. markets. The products were sold nationwide via Internet sales.
Source: <http://www.fda.gov/Safety/Recalls/ucm478794.htm>
11. *December 22, Reuters* – (National) **Costco E. coli outbreak appears to be over: CDC.** The U.S. Centers for Disease Control and Prevention reported December 22 that an E. coli outbreak linked to rotisserie chicken salad sold by Costco Wholesale Corporation was reportedly over after the outbreak began November 3 and sickened 19 people across 7 States. The source of the outbreak remains unknown.
Source: <http://www.reuters.com/article/us-costco-wholesale-ecoli-idUSKBN0U521N20151222>

For another story, see item [6](#)

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

12. *December 22, U.S. Food and Drug Administration* – (International) **CDER alert: FDA warns of potential contamination of drug shipments from explosions in Tianjin City.** The U.S. Food and Drug Administration issued an alert December 22 to drug compounders and manufacturers claiming that drug shipments from Tianjin, China, may be contaminated with chemicals following two large explosions at Tianjin Dongjiang Port Ruihai International Logistics Co., chemical warehouse in August. The alert was issued after regulators detected hydrogen cyanide in two shipments of drugs from Tianjin Tianyao Pharmaceuticals Co., Ltd. which is located 18 miles from the

explosion site.

Source: <http://www.fda.gov/Drugs/DrugSafety/ucm478170.htm>

13. *December 22, Round Rock Patch* – (Texas) **HealthSound Rehab Hospital warns of potential data breach.** HealthSouth Rehabilitation Hospital of Round Rock notified 1,359 patients December 22 that their personal and medical information may have been breached following an October theft of a password-protected laptop from an employee's vehicle. Officials continue to investigate the theft.
Source: <http://patch.com/texas/round-rock/healthsouth-rehab-hospital-warns-potential-data-breach-0>

Government Facilities Sector

Nothing to report

Emergency Services Sector

Nothing to report

Information Technology Sector

14. *December 23, SecurityWeek* – (International) **Recently patched NTP flaws affect Siemens RUGGEDCOM devices.** Siemens released an advisory stating that its industrial communications devices, running all versions ROX I and certain versions of ROX II operating systems (OS) had several previously patched network time protocol (NTP) vulnerabilities including an improper input validation issue, an authentication bypass issue, and a configured time server issue, among other flaws, that if exploited, can be reconfigured to use the NTP daemon from ntp.org for time synchronization in electric utility substations and traffic control cabinets. Siemens released firmware updates to address the flaws on ROX II devices and advised customers to use firewalls to block NTP packets from unknown sources, as well as use NTP time synchronization in trusted networks.
Source: <http://www.securityweek.com/recently-patched-ntp-flaws-affect-siemens-ruggedcom-devices>
15. *December 22, SecurityWeek* – (International) **RCE, SQLi flaws found in popular web apps.** Researchers from High-Tech Bridge discovered several vulnerabilities in popular web applications including various versions of osCmax application and osCommerce's Online Merchant store solution, Roundcube, Oclass, and SocialEngine that are susceptible to remote code execution (RCE), cross-site request forgery (CSRF) attacks, Structured Query Language (SQL) injection vulnerabilities, and path traversal vulnerabilities. Roundcube and Oclass developers are reportedly working to patch the vulnerabilities.
Source: <http://www.securityweek.com/rce-sqli-flaws-found-popular-web-apps>

For additional stories, see items [16](#) and [17](#)

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

16. *December 23, Softpedia* – (International) **Botnet of Aethra Routers used for Brute-Force WordPress Sites.** Security researchers from VoidSec discovered a botnet that used vulnerable Aethra Internet routers and modems to perform various reflected cross-site scripting (XSS) attacks, cross-site request forgery (CSRF) attacks, and brute-force attacks through six Internet Service Providers (ISP) including Fastweb, Albacom (BT-Italia), Clouditalia, Qcom, WIND, and BSI Assurance UK to compromise WordPress Web sites. The botnet easily accessed approximately 12,000 Aethra routers worldwide as the routers were still using their default login credentials.
Source: <http://news.softpedia.com/news/botnet-of-aethra-routers-used-for-brute-force-wordpress-sites-498028.shtml>

For another story, see item [14](#)

Commercial Facilities Sector

17. *December 23, Associated Press* – (International) **Hello Kitty owner Sanrio says fan site security leak fixed.** Sanrio Co., Ltd reported December 22 that it fixed a security vulnerability on an online fan Web site, SanrioTown.com after the personal information of 3.3 million users were compromised following a security researcher's discovery December 19 that names, birthdays, and encrypted passwords can be extracted by using multiple Internet Protocol (IP) addresses.
Source: <http://abcnews.go.com/Entertainment/wireStory/kitty-owner-sanrio-fan-site-security-leak-fixed-35918666>
18. *December 22, Portland Oregonian* – (Oregon) **Tigard police seize 470 iPhones related to gift card fraud.** Tigard police are investigating December 22 an organized retail theft scheme that occurred at the Washington Square Mall and Bridgeport Village after police stopped 2 men and found 470 Apple iPhones products worth \$292,000, as well as hundreds of fraudulent gift cards and receipts totaling \$585,000. Police confiscated the stolen items and believe that the counterfeit credit cards may have originated from southern California.
Source:
http://www.oregonlive.com/tigard/index.ssf/2015/12/tigard_police_seize_470_iphone.html

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.