Daily Open Source Infrastructure Report
11 September 2014

Top Stories

- A chemical reaction at the Havilland Enterprises, Inc. chemical facility in Grand Rapids, Michigan, September 9 created a vapor release that produced a large gas cloud above the building and led to the evacuation of nearby homes and businesses for over 3 hours.– *WOOD 8 Grand Rapids* (See item 2)
- Six individuals and six corporate entities were indicted September 9 for allegedly laundering around $500 million in proceeds from fraudulent securities transactions involving more than 100 U.S. citizens and residents– *U.S. Attorney's Office, Eastern District of New York* (See item 4)
- One northbound lane of Highway 101 in Carpinteria, California, was closed for 9 hours for investigation September 9 when the driver of a pickup truck entered a lane that was closed for construction and crashed into a construction truck, killing the driver of the pickup.– *KEYT 3 Santa Barbara* (See item 5)
- Sensys Networks, a company that manufactures sensor devices used in wireless traffic control systems, announced September 5 that it released software updates for its products to protect systems against attacks exploiting a lack of encryption or insufficient authentication methods.– *Securityweek* (See item 7)

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. *September 9, KHON 2 Honolulu* – (Hawaii) **Boiler leak caused issues at Waiau plant, power problem remains unsolved.** Hawaiian Electric reported that it discovered problems at its Kalaeloa and Waiau power plants during inspections September 6-7, which led to the utility asking customers on Oahu to conserve power September 8. One generator was repaired but a connection issue between the Kalaeloa plant and the grid remained unresolved and under investigation.
   Source: http://khon2.com/2014/09/09/boiler-leak-caused-issues-at-waiau-plant-power-problem-remains-unsolved/

[Return to top]

Chemical Industry Sector

2. *September 9, WOOD 8 Grand Rapids* – (Michigan) **2nd hazmat incident at Haviland this year.** A chemical reaction at the Havilland Enterprises, Inc. chemical facility in Grand Rapids September 9 created a vapor release that triggered the plant's sprinkler system and produced a large gas cloud above the building. An evacuation order for homes and businesses in the northwest area of the city was lifted over 3 hours later when authorities cleared the scene and determined the air quality to be safe.
   Source: http://woodtv.com/2014/09/09/grpd-hazmat-situation-at-haviland-industries/

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

3. *September 9, U.S. Department of Labor* – (Alabama) **Alabama metal manufacturer cited by OSHA for exposing workers to amputations, falls and other workplace safety hazards.** Diversified Fabricating Inc. was cited by the Occupational Safety and Health Administration September 9 for 23 safety and health violations at its Oneonta facility. Proposed fines totaled $73,500.
   Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26649

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

4. *September 9, U.S. Attorney's Office, Eastern District of New York* – (International) **Six corporate executives and six corporate entities indicted for orchestrating a $500 million offshore asset protection, securities fraud, and money laundering scheme.** Six individuals from the U.S., Canada, Belize, and the Bahamas and six corporate entities were indicted September 9 for allegedly operating an elaborate scheme to enable U.S. citizens to circumvent and evade securities and tax laws by setting up fake companies to evade taxes and engage in money laundering. The alleged scheme laundered around $500 million between 2009 and 2014.
   Source: http://www.fbi.gov/newyork/press-releases/2014/six-corporate-executives-and-six-corporate-entities-indicted-for-orchestrating-a-500-million-offshore-asset-protection-securities-fraud-and-money-laundering-scheme

For additional stories, see items **27** and **28**

[Return to top]

Transportation Systems Sector

5. *September 9, KEYT 3 Santa Barbara* – (California) **Santa Barbara man identified in fatal Highway 101 morning crash.** One northbound lane of Highway 101 in Carpinteria was closed for 9 hours for investigation September 9 when the driver of a pickup truck entered a lane that was closed for construction and crashed into a Granite Construction truck, killing the driver of the pickup.
   Source: http://www.keyt.com/news/one-man-dead-after-early-morning-crash-in-carpinteria/27932506

6. *September 9, KTVU 2 Oakland* – (California) **Suspicious device that shut down Hwy 12 was scavenging hunt prize.** A portion of State Highway 12 near Fairfield was shut down for over 2 hours September 9 after a suspected pipe bomb was found. A bomb squad responded to the scene and later determined the suspicious device to be a Geocaching apparatus used for a game.
   Source: http://www.ktvu.com/news/news/local/possible-pipe-bomb-prompts-shutdown-highway-12/nhJxf/

7. *September 9, Securityweek* – (International) **Vendor fixes vulnerabilities in wireless traffic sensors.** Sensys Networks, a company that manufactures sensor devices used in wireless traffic control systems, announced September 5 that it released software updates for its products to address security vulnerabilities and protect systems against attacks caused by lack of encryption or sufficient authentication methods. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory stating that the issues affect Sensys Networks VSN240-F and VSN240-T systems and advised operators to update their software installations.

Source: http://www.securityweek.com/vendor-fixes-vulnerabilities-wireless-traffic-sensors

[Return to top]

Food and Agriculture Sector

Nothing to report

[Return to top]

Water and Wastewater Systems Sector

8. *September 10, Associated Press* – (Minnesota) **Boil water order lifted in Brainerd.** A boil water advisory in Brainerd was lifted September 9 after 40 city-ordered water quality tests came back negative for bacteria. The advisory was issued after recent storms knocked out power to the city's water system, posing risk for contamination.
   Source: http://www.winonadailynews.com/news/state-and-regional/mn/boil-water-order-lifted-in-brainerd/article_b763137c-869b-5f30-9214-351de8f0699e.html

9. *September 9, WEYI 25 Saginaw* – (Michigan) **Boil water advisory lifted and residents react.** Officials lifted a boil water advisory for residents and businesses in Flint September 9 when test results showed the water supply was clear of bacterial contaminants after routine water tests September 5 revealed the presence of coliform bacteria.
   Source: http://www.minbcnews.com/news/story.aspx?id=1094576

10. *September 9, Peninsula Daily News* – (Washington) **Advisory to be lifted today against contract with Port Angeles Harbor waters.** An advisory warning against recreational contract with the water of Port Angeles Harbor was lifted September 9 following a sewage spill September 2 in which 1 million gallons of partially treated sewage spilled into the water due to a malfunction at the city's sewage treatment plant.
    Source: http://www.peninsuladailynews.com/article/20140910/NEWS/309109994/advisory-to-be-lifted-today-against-contact-with-port-angeles-harbor

[Return to top]

Healthcare and Public Health Sector

11. *September 9, U.S. Department of Labor* – (Michigan) **US Department of Labor's OSHA finds 6 safety, health violations at Saginaw, Michigan, medical center for veterans.** The Occupational Safety and Health Administration cited the Aleda E. Lutz Veterans Administration Medical Center in Saginaw with one repeat and five serious violations for exposing workers to hazards including asbestos, bloodborne pathogens, and the unsafe operation of powered vehicles.
    Source:

https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=26652

12. *September 9, WDHN 21 Dothan* – (Alabama) **Man indicted for stealing patient records from Flowers Hospital.** A Henry County man was indicted September 9 for allegedly stealing and selling the personal information of patients at Flowers Hospital between June 2013 and February 2014. The former Flowers Hospital employee previously pleaded guilty to similar federal charges.
Source: http://www.dothanfirst.com/story/d/story/court-records-show-a-grand-jury-that-recent-met-in/28832/gjGtM4LrS0SMNsmo0KCjjQ

[Return to top]

Government Facilities Sector

13. *September 10, WFLA 8 Tampa* – (Florida) **Hillsborough school bus crash sends 21 to hospital.** Two school buses en route to Eisenhower Middle School collided when one bus rear-ended the second in Hillsborough County September 10, sending 19 students and both drivers to area hospitals.
Source: http://www.wfla.com/story/26495468/crash-involving-2-hillsborough-school-buses-injuries-reported

14. *September 9, Softpedia* – (International) **Compromised Web server exposes personal info at California State University, East Bay.** California State University, East Bay officials notified over 6,000 employees and former students that a security breach was detected during a routine inspection August 11 and that an attacker used malware to access a Web server and extract files containing personal information, including full names and Social Security numbers. The university removed the malware from its systems and mitigated server vulnerabilities.
Source: http://news.softpedia.com/news/Compromised-Web-Server-Exposes-Personal-Info-At-California-State-University-East-Bay-458268.shtml

15. *September 9, WCAL 9 Los Angeles* – (California) **Aliso Viejo school closed through Wednesday due to threat.** Classes at the St. Mary of All Angels campus in Aliso Viejo were cancelled September 9 through September 10 after school administrators received a threatening email September 8. Authorities are investigating the incident.
Source: http://losangeles.cbslocal.com/2014/09/09/aliso-viejo-school-closed-through-wednesday-due-to-threat/

16. *September 9, Alexandria Town Talk* – (Louisiana) **Four Rapides schools get bomb threats Tuesday.** Police are investigating after four middle and high schools in Rapides Parish received phoned bomb threats September 9, prompting the evacuation of each building. The facilities were searched and cleared after no devices were found.
Source: http://www.thetowntalk.com/story/news/local/2014/09/09/bomb-threat-ash-police-alexandria/15335549/

17. *September 9, WJLA 7 Washington, D.C.* – (Maryland) **School bus crash with car**

injures seven in Upper Marlboro. A school bus and a car were involved in an accident in Upper Marlboro September 9, injuring both drivers and five students. Source: http://www.wjla.com/articles/2014/09/school-bus-crash-with-car-injures-seven-in-upper-marlboro-106956.html

For another story, see item **11**

[Return to top]

Emergency Services Sector

18. *September 8, WUSA 9 Washington D.C.* – (Washington D.C.) **7 DC ladder trucks fail inspection.** The District of Columbia Fire and Emergency Medical Services Department announced in a statement September 8 that an inspection revealed that 7 of the 17 ladder trucks with the D.C. fire department failed inspection due to varying degrees of rust at the base of their ladder supports and were taken out of service. Source: http://www.wusa9.com/story/news/2014/09/08/dc-fire-ladder-trucks-fail-inspection/15282771/

[Return to top]

Information Technology Sector

19. *September 9, IDG News Service* – (International) **Adobe fixes critical flaws in Flash Player, delays Reader and Acrobat updates.** Adobe Systems released a critical security update for its Flash Player software, closing 12 security issues, 9 of which could lead to remote code execution. The company also delayed planned patches for Reader and Acrobat by 1 week due to issues identified during testing. Source: http://www.networkworld.com/article/2604961/adobe-fixes-critical-flaws-in-flash-player-delays-reader-and-acrobat-updates.html

20. *September 9, Network World* – (International) **September Patch Tuesday: Microsoft closes door on IE zero day attacks.** Microsoft released its monthly Patch Tuesday round of updates for September, with 4 bulletins closing 42 vulnerabilities in various Microsoft products. One bulletin for the Internet Explorer browser closes 37 vulnerabilities, 1 of which was a critical Internet Explorer zero-day vulnerability. Source: http://www.networkworld.com/article/2604465/microsoft-subnet/september-patch-tuesday-microsoft-closes-door-on-ie-zero-day-attacks.html

21. *September 9, The Register* – (International) **Use home networking kit? DDoS bot is BACK…and it has EVOLVED.** A researcher identified a new variant of the Lightaidra router-to-router malware that targets consumer-grade cable and DSL modems using default passwords in order to use them in distributed denial of service (DDoS) attacks. The new variant is able to reconfigure victims' firewalls and requires Linux to be running on targeted devices in order to infect them. Source: http://www.theregister.co.uk/2014/09/09/linux_modem_bot/

22. *September 9, Softpedia* – (International) **Apple beefs up security, sends iCloud access alert.** Apple announced September 5 that within 2 weeks it would implement new security policies for its iCloud service following attacks that leaked personal photos belonging to celebrities. Some features have already been implemented, such as a notification when an iCloud account is accessed via a Web browser.
Source: http://news.softpedia.com/news/Apple-Beefs-Up-Security-Sends-iCloud-Access-Alert-458282.shtml

23. *September 9, The Register* – (International) **Phishing miscreants are THWARTING secure-sleuths with AES crypto.** Researchers with Symantec identified what they believe was the first use of AES encryption to disguise fraudulent Web sites designed to steal users' login credentials. The use of AES encryption allows attackers to make the analysis of phishing sites more difficult without affecting how the sites appear and function to users.
Source:
http://www.theregister.co.uk/2014/09/09/phishing_scam_uses_aes_crypto_to_hide/

For another story, see item **7**

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

[Return to top]

Communications Sector

24. *September 8, KTVZ 21 Bend* – (Oregon) **BendBroadband restoring TV service after outage.** Television service was disrupted for BendBroadband customers in Oregon September 8 for nearly 13 hours when one of the aggregation routers failed a routine boot, causing the outage.
Source: http://www.ktvz.com/news/bendbroadband-hit-by-lengthy-tv-outage/27941216

25. *September 9, Paris Beacon-News* – (Illinois) **Westville accident left Paris residents without cable, internet.** Approximately 2,200 NewWave Communications customers in Paris, Illinois, experienced cable, phone, and Internet disruptions for 5 hours when a fiber vault was destroyed by a tractor.
Source: http://www.parisbeacon.com/news/article_f169676c-3835-11e4-b44f-001a4bcf887a.html

[Return to top]

Commercial Facilities Sector

26. *September 10, Associated Press* – (Kansas) **Residents evacuated as roof collapses during apartment fire.** Residents from 16 units at the Aspen Lodge Apartments complex in Overland Park were displaced by a September 10 fire that caused the structure's roof to collapse.
Source: http://salinapost.com/2014/09/10/residents-evacuated-as-roof-collapses-during-apartment-fire/

27. *September 9, WTVT 13 Tampa* – (Florida) **Police: Beef O' Brady's electronic payment network hacked.** Police reported that the electronic payment network of four Beef O' Brady's restaurants in Florida was breached and customers' payment card information was stolen. The company has taken steps to ensure the security of the systems since the issue was identified.
Source: http://www.myfoxtampabay.com/story/26486959/police-beef-o-bradys-electronic-payment-network-hacked

28. *September 9, Softpedia* – (International) **Yandy.com hacked, financial information exposed.** Yandy.com notified its customers that a Web-based database hosting customers' information, including payment card data, was accessed by an unknown party at least four times between May 28 and August 18. The online retailer detected the breach August 18 and has implemented additional measures to secure its systems.
Source: http://news.softpedia.com/news/Yandy-com-Hacked-Financial-Information-Exposed-458255.shtml

[Return to top]

Dams Sector

Nothing to report

[Return to top]

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.