Daily Open Source Infrastructure Report
08 August 2014

Top Stories

- Researchers at the Black Hat 2014 conference presented findings that showed how attackers could remotely compromise the systems of certain vehicles that integrate Bluetooth, radio, or other communications methods into their sensors and controls. – *Threatpost* (See item **5**)
- A Qualys researcher discovered two devices, the Morpho Detection Itemiser 3 and the Kronos 4500, used at U.S. airports and other security checkpoints have backdoors in which hackers can access usernames and passwords to the devices. – *Dark Reading* (See item **11**)
- DHS and the U.S. Office of Personnel Management (OPM) suspended work with US Investigations Services (USIS) August 6 after the contractor reported a cyber-attack likely involving the theft of personal information of DHS employees. – *Reuters* (See item **19**)
- At least 600 guests and residents from three hotels in Vail, Colorado, were evacuated for approximately 8 hours August 6 after a construction crew inadvertently struck a large steel natural gas pipe and caused a leak. – *KUSA 9 Denver* (See item **30**)

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. *August 7, Forum of Fargo-Moorhead* – (North Dakota) **Oil, brine spill released into slough.** Taqa North USA reported that about 100 barrels of brine and oil were released into a slough near Lignite in Burke County from a main injection line feeding three injection wells. Health inspectors responded to the site to monitor cleanup and response efforts.
   Source: http://www.jamestownsun.com/content/oil-brine-spill-released-slough

2. *August 6, Pittsburgh Tribune-Review* – (Pennsylvania) **State points to human error, bad communication in fatal Chevron well fire.** The Pennsylvania Department of Environmental Protection released two reports August 6 claiming human error by an unsupervised employee of contractor Cameron International Corp., likely caused the February 11 fatal incident on the Lanco well pad in Dunkard that killed a field service technician after a leak caused a fire on the Chevron-owned gas well in Greene County.
   Source: http://triblive.com/news/adminpage/6569001-74/chevron-dep-state

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *August 7, Nuclear Street* – (Illinois) **Safety system trips La Salle reactor.** The Unit 2 reactor at the La Salle nuclear power plant in Illinois shut down automatically August 5 when a safety system activated unexpectedly. The operators of the plant are investigating the cause of the safety system activation.
   Source:
   http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2014/08/07/safety-system-trips-la-salle-reactor-080702.aspx

[Return to top]

Critical Manufacturing Sector

4. *August 7, U.S. Consumer Product Safety Commission* – (National) **VIZIO recalls to repair 39- and 42-inch E-Series flat panel televisions due to risk of tip over.** VIZIO announced a recall August 6 for around 245,000 E-Series 39-inch and 42-inch televisions due to the potential for the televisions' stands to fail and tip over unexpectedly.
   Source: http://www.cpsc.gov/en/Recalls/2014/VIZIO-Recalls-to-Repair-39-and-42-Inch-E-Series-Flat-Panel-Televisions/

5. *August 6, Threatpost* – (International) **Car hacking enters remote exploitation phase.** Researchers at the Black Hat 2014 conference presented findings that showed how attackers could remotely compromise the systems of certain vehicles that integrate Bluetooth, radio, or other communications methods into their sensors and controls. Among the most vulnerable types of systems the researchers found were systems that can control vehicles automatically, such as active lane control, self-parking, and pre-collision systems.
Source: http://threatpost.com/car-hacking-enters-remote-exploitation-phase

6. *August 6, Motor Trend* – (National) **184,611 GM SUV models recalled for power window short.** General Motors announced a recall for 184,611 model year 2005-2007 Buick Rainier, Chevrolet Trailblazer, GMC Envoy, Isuzu Ascender, and Saab 9-7x vehicles due to the potential for fluid to enter the driver's door master power window switch module, which could lead to lack of window function or smoldering and fire.
Source: http://wot.motortrend.com/1408_184611_gm_suv_models_recalled_for_power_window_short.html

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

7. *August 6, Minneapolis/St. Paul Business Journal* – (Minnesota; Arizona; Indiana) **Charges: Eden Prairie investment adviser spent funds from $13M Ponzi scheme at casinos, strip clubs.** The Minnesota U.S. Attorney's Office filed charges against an Eden Prairie, Minnesota financial planner for allegedly using his company, Meadows Financial Group, to run a Ponzi scheme that collected at least $13 million from over 50 clients in Minnesota, Arizona, and Indiana. The charges allege that the man used most of the investment funds to pay existing investors and for personal use.
Source: http://www.bizjournals.com/twincities/blog/law/2014/08/charges-eden-prairie-investment-adviser-spent-13m.html

8. *August 6, Los Angeles Times* – (California) **'Hills Bandit' of O.C. robs bank in Carlsbad, FBI says.** The FBI stated that a suspect known as the "Hills Bandit" robbed a U.S. Bank branch in Carlsbad, California, August 5. The man is also suspected of previously robbing three other banks in Orange County.
Source: http://www.latimes.com/local/lanow/la-me-ln-bank-robber-carlsbad-20140806-story.html

9. *August 6, Salt Lake Tribune* – (Utah) **Jury finds fraudster guilty in commodities trading scam.** The former head of Utah-based U.S. Ventures was found guilty August

6 on 5 counts of fraud and of filing a false tax return for running his company as a Ponzi scheme that lost $10.5 million in investments and paid out funds to previous investors and for the man's personal use.
Source: http://www.sltrib.com/sltrib/news/58269048-78/holloway-jury-money-murphy.html.csp

[Return to top]

Transportation Systems Sector

10. *August 7, Delaware County Daily Times* – (Pennsylvania) **Natural gas leak forces brief closure of shipping along Delaware River.** A U.S. Army Corps of Engineers dredging vessel struck an 8-inch pipeline near Little Tinicum Island in Pennsylvania causing a natural gas leak at the bottom of the Delaware River August 4 which prompted authorities to close the shipping channel for 75 minutes while they inspected the leak. The PBF Energy-owned main natural gas pipeline was shut down and repaired during the closure.
Source: http://www.delcotimes.com/general-news/20140806/natural-gas-leak-forces-brief-closure-of-shipping-along-delaware-river

11. *August 6, Dark Reading* – (International) **TSA checkpoint systems found exposed on the net.** A Qualys researcher discovered two devices, the Morpho Detection Itemiser 3 and the Kronos 4500, used at U.S. airports and other security checkpoints have backdoors in which hackers can access usernames and passwords to the devices. The researchers also found about 6,000 Kronos time clock systems that are online and open to the public, two of which are located at U.S. airports.
Source: http://www.darkreading.com/vulnerabilities---threats/advanced-threats/tsa-checkpoint-systems-found-exposed-on-the-net/d/d-id/1297843

12. *August 6, Kennewick Tri-City Herald* – (Washington) **Delays on Highway 730 near Umatilla likely as derailment repairs continue.** Crews will close lanes and detour traffic for repair work along Highway 730 near the Oregon-Washington border in Umatilla through August 22 after a train derailment the week of July 28 damaged the railroad tracks.
Source: http://www.tri-cityherald.com/2014/08/06/3095267/delays-on-highway-730-near-umatilla.html

For another story, see item **20**

[Return to top]

Food and Agriculture Sector

13. *August 6, WEWS 5 Cleveland* – (Ohio) **Owner of Sandusky winery indicted for actions related to government-backed farm loans.** The owner and operator of Kraus Winery, Inc., in Sandusky, Ohio, was indicted August 6 on five federal charges related to the securing and repayment of loans for the winery. The New York man allegedly

sold about $2 million in grapes and wine that were pledged as collateral for federal loans, totaling $594,870, and failed to remit the proceeds from the sales.
Source: http://www.newsnet5.com/news/local-news/oh-erie/owner-of-sandusky-winery-indicted-for-actions-related-to-government-backed-farm-loans

14. *August 6, Miami Herald* – (Florida) **Third arrest in illegal Miami-Dade slaughterhouse case.** Authorities arrested a Florida man and charged him with 30 counts of animal cruelty August 5 in connection with an illegal West Miami-Dade slaughterhouse after an undercover investigation revealed the slaughtering of animals in a cruel and painful manner. Two others were arrested and charged on similar counts in March and April, and the previous operators were issued code violations in November that were not addressed.
Source: http://www.miamiherald.com/2014/08/06/4274692/third-arrest-in-illegal-miami.html

15. *August 6, U.S. Department of Agriculture* – (National) **New York firm recalls sausage product due to misbranding and undeclared allergen.** The Food Safety and Inspection Service announced August 6 that Zemco Industries Inc., issued a recall for about 106,800 pounds of its Cavanaugh Smoked Sausage due to misbranding and undeclared soy. The product was sold in 2.5-pound packages and sent to distribution centers and retailers nationwide.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2014/recall-050-2014-release

16. *August 6, Foods Safety News* – (Washington) **Vibrio illnesses prompt closure of Samish Bay's oyster harvest until Sept. 30.** State health officials closed commercial oyster harvesting in Washington's Samish Bay until September 30 after confirming shellfish from the bay was the source of at least one illness, and possibly three others, caused by bacterium Vibrio parahaemolyticus. Clam, mussel, and geoduck harvests were not impacted by the closure.
Source: http://www.foodsafetynews.com/2014/08/illnesses-prompt-wa-to-close-samish-bays-oyster-harvest-until-sept-30

For another story, see item **34**

[Return to top]

Water and Wastewater Systems Sector

17. *August 7, WNWO 24 Toledo* – (Ohio) **New boil water advisory confuses Toledo residents in wake of H2O crisis.** A boil water advisory was issued to some residents in Toledo August 5 and expected to expire August 8 due to repairs to the city's water distribution system.
Source: http://www.nbc24.com/news/story.aspx?id=1080330

18. *August 5, Beaufort County Island Packet* – (South Carolina) **5,000 gallons of sewage leak into Battery Creek.** A leaking sewer line discovered August 4 released over

5,000 gallons of untreated sewage into the marshes of Battery Creek near Shell Point, prompting authorities to issue a swimming advisory for the creek and its tributaries. The county's water authority made temporary repairs to the line while crews worked to make permanent repairs, line upgrades, and test the water.
Source: http://www.islandpacket.com/2014/08/05/3243267/5000-plus-gallons-of-sewage-leak.html

[Return to top]

Healthcare and Public Health Sector

Nothing to report

[Return to top]

Government Facilities Sector

19. *August 7, Reuters* – (National) **U.S. Homeland Security contractor reports computer breach.** DHS and the U.S. Office of Personnel Management (OPM) suspended work with Virginia-based US Investigations Services (USIS) after the contractor reported a cyberattack likely involving the theft of personal information of DHS employees. DHS notified its entire workforce and is working with OPM, FBI, and USIS to determine the scope of the intrusion.
Source: http://www.reuters.com/article/2014/08/07/us-usa-security-contractor-idUSKBN0G62N420140807

20. *August 7, Associated Press* – (Oregon; California) **275 households told to flee Oregon wildfire.** An additional 275 homes were ordered to evacuate August 6 due to a new wildfire along Columbia River Gorge in Rowena while crews throughout Oregon battled 10 other large wildfires which have burned tens of thousands of acres and prompted the evacuation of dozens of homes and the closure of a portion of U.S. Highway 30.
Source: http://news.msn.com/us/275-households-told-to-flee-oregon-wildfire

21. *August 6, Boise State Public Radio* – (Idaho) **North Idaho's Big Cougar Fire grows to 47 square miles, evacuation orders in place.** Officials ordered voluntary evacuations for residents living from China Garden to Captain John Creek in Idaho August 6 due to the 30,000-acre Big Cougar Fire while residents in Getta Creek were under mandatory evacuation orders due to the 2,600-acre Highrange Fire.
Source: http://boisestatepublicradio.org/post/north-idahos-big-cougar-fire-grows-47-square-miles-evacuation-orders-place

[Return to top]

Emergency Services Sector

22. *August 7, WCAX 3 Burlington* – (Vermont) **Vermont 911 system experiences**

statewide outage. Emergency 9-1-1 service was down for about 45 minutes Statewide in Vermont August 6. Officials are investigating the cause of the outage and the Colorado-based company that runs Vermont's 9-1-1 system.
Source: http://wwlp.com/2014/08/07/vermont-911-system-experiences-statewide-outage/

23. *August 6, WKYC 3 Cleveland* – (Ohio) **Elyria: Power outage keeps Lorain County Justice Center closed.** A power outage prompted the closure of the Lorain County Justice Center in Elyria August 6. Crews restored power and the center was scheduled to reopen August 7.
Source: http://www.wkyc.com/story/news/local/lorain-county/2014/08/06/power-outage-closes-lorain-county-justice-center/13662455/

[Return to top]

Information Technology Sector

24. *August 7, Help Net Security* – (International) **Symantec issues update fixing Endpoint Protection zero-day.** Symantec issued a patch for its Symantec Endpoint Protection (SEP) security solution to address a zero-day vulnerability identified by Offensive Security researchers that could allow an attacker with access to the target computer to escalate admin privileges or cause a denial of service (DoS) situation. The vulnerability can not be exploited remotely but the exploit code is publicly available.
Source: http://www.net-security.org/secworld.php?id=17218

25. *August 7, Softpedia* – (International) **OpenSSL receives nine security fixes.** A new version of the OpenSSL library was released, closing nine security vulnerabilities identified by researchers from various organizations. The vulnerabilities could lead to information leaking, downgrading to lower versions of the security protocol, or denial of service (DoS) attacks.
Source: http://news.softpedia.com/news/OpenSSL-Receives-Nine-Critical-Fixes-453932.shtml

26. *August 7, Softpedia* – (International) **US Plextor website hacked by CoMoDo Islamic hackers.** Attackers identifying themselves as the CoMoDo group defaced the Web site of computer hardware manufacturer Plextor Americas. The company stated that they are investigating the incident.
Source: http://news.softpedia.com/news/US-Plextor-Website-Hacked-by-CoMoDo-Islamic-Hackers-453960.shtml

27. *August 7, Softpedia* – (International) **WordPress and Drupal fix common PHP XML parser vulnerability.** WordPress and Drupal released new versions of their respective products in a joint effort to close an XML processing vulnerability that existed in both services and could be used by attackers to perform denial of service (DoS) attacks. The vulnerability was reported by a researcher at Salesforce.com and affected over 250 million Web sites according to Incapsula researchers.
Source: http://news.softpedia.com/news/WordPress-and-Drupal-Fix-Common-PHP-

XML-Parser-Vulnerability-453888.shtml

28. *August 6, Securityweek* – (International) **APT group hijacks popular domains to mask C&C communications: FireEye.** Researchers with FireEye reported identifying an advanced persistent threat campaign dubbed "Poisoned Hurricane" that used a variant of the PlugX (Kaba) malware configured to resolve DNS lookups through the nameservers of Hurricane Electric, which then spoofed legitimate domains and IP addresses to disguise the malware's communication with command and control (C&C) servers.
Source: http://www.securityweek.com/apt-group-hijacks-popular-domains-mask-cc-communications-fireeye

29. *August 6, Softpedia* – (International) **Twitter URL shortening service abused by spammers.** Cloudmark researchers reported that the t.co URL shortening service used by Twitter was used in 54 percent of shortened links blacklisted by the company for use in spam campaigns, and that one entity appeared to be behind two observed campaigns abusing the service, among other findings.
Source: http://news.softpedia.com/news/Twitter-URL-Shortening-Service-Abused-by-Spammers-453832.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

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

30. *August 7, KUSA 9 Denver* – (Colorado) **Vail gas leak repaired, evacuees allowed to return.** At least 600 guests and residents from three hotels in Vail, Colorado, were evacuated August 6 after a construction crew inadvertently struck a large steel natural gas pipe and caused a leak. The leak was repaired and guests were allowed to return to their hotels after about 8 hours.
Source: http://www.9news.com/story/news/local/2014/08/06/600-people-evacuated-after-gas-leak/13697433/

31. *August 7, The Register* – (International) **Cracker takes control of 200 rooms in Chinese hotel.** A security consultant revealed during the Black Hat 2014 conference

that he was able to remotely control amenities in over 200 rooms at a luxury hotel in China due to an insecure automation protocol that is commonly used in China and Europe. Prior to the conference, the researcher alerted the hotel's parent company and the system flaw was corrected.
Source:
http://www.theregister.co.uk/2014/08/07/cracker_takes_control_of_200_rooms_in_chinese_hotel/

32. *August 6, Reuters* – (Texas) **Fifty stranded passengers rescued after Dallas zoo ride stalls.** Officials used ladders to evacuate about 50 patrons from a passenger monorail at the Dallas Zoo August 6 after an electrical power surge stalled the train and stranded passengers 12 feet in the air for about 30 minutes. Officials closed the monorail until at least August 8 to assess the damage and determine the source of the surge.
Source: http://www.reuters.com/article/2014/08/06/us-usa-dallas-zoo-idUSKBN0G62DA20140806

33. *August 5, Pittsburgh Tribune-Review* – (Ohio) **Feds seize half-million in bogus goods at flea market.** Immigration and Customs Enforcement agency officials announced August 5 that more than $500,000 worth of counterfeit merchandise was seized from about 15 vendors during a July 25 raid of the Rogers Community Auction in Ohio.
Source: http://triblive.com/news/adminpage/6563986-74/rogers-vendors-goods

[Return to top]

Dams Sector

34. *August 6, KTVA 11 Anchorage* – (International) **Canadian dam fails, over 1 billion gallons of wastewater spilled.** Over 1 billion gallons of wastewater was released from the Mount Polley tailings pond dam in British Columbia, Canada, August 4 prompting an indefinite water ban for a nearby community and raising salmon concerns for Alaska fishermen.
Source: http://www.ktva.com/canadian-dam-fails-over-1-billion-gallons-of-wastewater-spilled-974/

[Return to top]

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