Daily Open Source Infrastructure Report
25 August 2016

Top Stories

- Ford Motor Company issued a recall August 24 for 77,502 of its model years 2013 – 2015 vehicles in select makes due to faulty fuel pump control modules, which may fail and cause the engine to stall while the vehicle is in motion. – *TheCarConnection.com* (See item 2)
- Four private equity fund advisers affiliated with Apollo Global Management, LLC agreed August 23 to pay $52.7 million to settle charges that the advisers misled investors and failed to monitor a senior partner who charged personal expenses to Apollo-advised funds. – *U.S. Securities and Exchange Commission* (See item 3)
- Four people were arrested in Murfreesboro, Tennessee, August 17 when police discovered 83 magnetic strips in the suspects' vehicle. – *WGNS 1450 AM Murfreesboro* (See item 4)
- Researchers warned that the Navis WebAccess component of the Navis maritime transportation logistics software suite was plagued by a zero-day structured query language (SQL) injection flaw after U.S. ports suffered cyber-attacks. – *Softpedia* (See item 7)

Fast Jump Menu

Energy Sector

1. *August 24, WOWT 6 Omaha*– (Nebraska) **Nearly 8,000 remain without power due to storms.** Nearly 8,000 Omaha Public Power District customers remained without power August 24 following heavy storms that knocked out power to approximately 21,500 customers in the Omaha, Nebraska metropolitan area August 23.
Source: http://www.wowt.com/content/news/OPPD-reports-16000-without-power-391114481.html

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

2. *August 24, TheCarConnection.com* – (National) **Recalls: 2017 Ford Escape; 2013-15 Ford Flex, Taurus, Lincoln MKS, MKT; 2015-16 Ford Transit.** Ford Motor Company issued a recall August 24 for 77,502 of its model years 2013 – 2015 vehicles in select makes sold in the U.S. due to a faulty fuel pump control module which may fail and cause the engine to stall or shut off while the vehicle is in motion, thereby increasing the risk of an accident. Ford also issued a recall for 17,985 of its model year 2017 Ford Escape vehicles sold in the U.S. due to faulty software that can cause the power windows to close with excessive force, thereby increasing the risk of injury.
Source: http://www.thecarconnection.com/news/1105732_recalls-2017-ford-escape-2013-15-ford-flex-taurus-lincoln-mks-mkt-2015-16-ford-transit

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *August 23, U.S. Securities and Exchange Commission* – (National) **Apollo charged with disclosure and supervisory failures.** The U.S. Securities and Exchange Commission announced August 23 that 4 private equity fund advisers affiliated with Apollo Global Management, LLC agreed to pay a $52.7 million settlement to resolve claims that the Apollo advisers failed to adequately inform investors about accelerated monitoring fees and benefits the advisers received, failed to disclose information regarding interest payments made on a loan between an adviser's affiliated general partner and 5 funds, and failed to monitor a senior partner who charged personal expenses to Apollo-advised funds and their portfolio companies.
Source: https://www.sec.gov/news/pressrelease/2016-165.html

4. *August 23, WGNS 1450 AM Murfreesboro* – (Tennessee) **Four arrested in fraudulent credit card case in Murfreesboro.** Four people were arrested in Murfreesboro, Tennessee, August 17 when police discovered 83 magnetic strips in the suspects' vehicle after the group allegedly used re-encoded credit cards at an area Walmart store to make multiple fraudulent purchases.
Source: http://wgnsradio.com/four-arrested-in-fraudulent-credit-card-case-in-murfreesboro--cms-34556

Transportation Systems Sector

5. *August 24, Harrisburg Patriot-News* – (Pennsylvania) **Traffic Alert: Crash shuts down I-81 in Franklin County.** North and southbound lanes of Interstate 81 in Franklin County, Pennsylvania, were closed for several hours August 23 while crews investigated the scene of a multi-vehicle crash.
Source: http://www.pennlive.com/news/2016/08/traffic_alert_44.html

6. *August 24, KCBS 2 Los Angeles* – (California) **Crash involving 3 big rigs snarls traffic on 710 Freeway in Long Beach.** All southbound lanes of the 710 Freeway in Long Beach, California, were closed for more than 7 hours August 24 while officials investigated a crash involving 3 semi-trucks that spilled diesel across the roadway. Two people were transported to an area hospital.
Source: http://losangeles.cbslocal.com/2016/08/24/big-rig-crash-long-beach-2/

7. *August 23, Softpedia* – (International) **US ports targeted with zero-day SQL injection flaw.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned that the Navis WebAccess component of the Navis maritime transportation logistics software suite was plagued by a zero-day structured query language (SQL) injection flaw after U.S. ports reported a series of attacks that targeted publicly available news-pages in the Navis application and occurred as a part of the Uniform Resource Locator (URL) string due to a flaw in the application's error reporting system. Navis released a patch for the flaw and ICS-CERT stated all five U.S. companies using the application have applied the necessary patches.
Source: http://news.softpedia.com/news/us-ports-targeted-with-zero-day-sql-injection-flaw-507566.shtml

8. *August 23, Abilene Reporter-News* – (Texas) **Highway 36 reopens southeast of Abilene.** Officials closed State Highway 36 near Abilene, Texas, for about 10 hours August 23 while crews worked to clear the wreckage after a semi-truck struck a concrete barrier and overturned, spilling fuel and its load of pipe across the roadway. No injuries were reported.
Source: http://www.reporternews.com/traffic/highway-36-reopens-southeast-of-abilene-3abea077-d010-2e08-e053-0100007f330e-391101101.html

9. *August 23, KLIX 1310 AM Twin Falls* – (Idaho) **Hailey garbage truck overturns on Highway 75.** Highway 75 in Hailey, Idaho, was closed for nearly 2 hours August 22 as crews worked to clear the wreckage after a garbage truck overturned and spilled oil

across the highway when the driver swerved to avoid hitting a motorcycle.
Source: http://newsradio1310.com/hailey-garbage-truck-overturns-on-highway-75/

10. *August 23, Enid News & Eagle* – (Oklahoma) **One critical after semi overturns, blocking Oklahoma 58 for hours.** Highway 51A near Fairview, Oklahoma, was closed for several hours August 22 while officials cleared the wreckage after a semi-truck overturned. Two people were sent to area hospitals with injuries.
Source: http://www.enidnews.com/news/one-critical-after-semi-overturns-blocking-oklahoma-for-hours/article_bc517fa6-693e-11e6-a03e-b7f8218429f1.html

11. *August 23, WTOV 9 Steubenville* – (Ohio) **U.S. 22 open after semi-truck rollover.** Highway 22 near Cadiz, Ohio, was closed for several hours August 23 after a semi-truck overturned and spilled a clear liquid substance and dust on the roadway. No injuries were reported.
Source: http://wtov9.com/news/local/us-22-open-after-semi-truck-rollover

12. *August 23, Westside Eagle Observer* – (Arkansas) **Truck accident closes Arkansas Highway 59 south of Gravette.** Highway 59 south of Gravette, Arkansas, was closed for several hours August 23 while crews worked to clean up the wreckage after 2 semi-trucks collided, causing a load of dog food to spill across the highway.
Source: http://www.eagleobserver.com/news/2016/aug/23/truck-accident-closes-arkansas-highway-59-south-gr/

Food and Agriculture Sector

13. *August 23, U.S. Food and Drug Administration* – (National) **Baptista's Bakery issues allergy alert on undeclared milk in Snack Factory Original Pretzel Crisps.** Baptista's Bakery, Inc. issued a voluntary recall August 17 for select lots of its Snack Factory Original Pretzel Crisps and Snack Factory Sriracha Lime Pretzel Crisps products sold in 7.2-ounce packages due to undeclared milk ingredients after it was discovered that products seasoned with milk ingredients were produced in the same facility as the recalled products. No illnesses have been reported.
Source: http://www.fda.gov/Safety/Recalls/ucm517720.htm

Water and Wastewater Systems Sector

See item **15**

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

14. *August 24, KIFI 8 Idaho Falls/KIDK 3 Idaho Falls* – (Idaho) **Henry's Creek fire grows to over 43,000 acres.** Crews reached 15 percent containment August 23 of the 43,235-acre Henry's Creek Fire burning in Bonneville County, Idaho, prompting

officials to issue an evacuation order for the Sunnyside/Bone area to Kepps Crossing.
Source: http://www.localnews8.com/news/henrys-creek-fire-grows-to-over-17000-acres/41329198

15. *August 23, WVIT 30 New Britain* – (Connecticut) **5 swimming areas closed today.** Connecticut Department of Energy and Environmental Protection officials released its area water quality report August 23, which stated that swimming areas at Silver Sands State Park in Milford, Indian Well State Park in Shelton, and Kettletown State Park in Southbury, as well as at 2 other State parks were closed after storm runoff caused elevated levels of bacteria in the water.
Source: http://www.nbcconnecticut.com/news/local/5-Swimming-Areas-Closed-Today-391034131.html

16. *August 23, KSTU 13 Salt Lake City* – (Idaho) **Fire crews respond to 2,000-acre grass fire near Idaho-Utah border.** Crews worked August 23 to contain a 2,000-acre grass fire burning in Franklin County, Idaho, which prompted the evacuation of Clifton residents.
Source: http://fox13now.com/2016/08/23/fire-crews-respond-to-grass-fire-near-idaho-utah-border/

Emergency Services Sector

Nothing to report

Information Technology Sector

17. *August 24, Help Net Security* – (International) **Leaked EXTRABACON exploit can work on newer Cisco ASA firewalls.** Researchers from SilentSignal discovered the EXTRABACON exploit of the zero-day buffer overflow vulnerability affecting the Simple Network Management Protocol (SNMP) code of the Cisco Adaptive Security Appliance (ASA), Private Internet eXchange (PIX), and Firewall Services Module versions 8.4. (4) and earlier leaked by ShadowBrokers, can also be modified to compromise ASA version 9.2.(4). Cisco researchers are working to develop a definite solution of the exploit.
Source: https://www.helpnetsecurity.com/2016/08/24/extrabacon-newer-cisco-asa/

18. *August 23, Softpedia* – (International) **Two free decrypters available for WildFire ransomware.** Kaspersky and Intel McAfee released two decrypters that can unclock files encrypted by WildFire ransomware infections and are available for download from the NoMoreRansom Website. Researchers stated that since July 23, WildFire infected 5,309 devices and earned 136 Bitcoin, or $79,000 from users paying the ransom.
Source: http://news.softpedia.com/news/two-free-decrypters-available-for-wildfire-ransomware-507572.shtml

19. *August 23, Softpedia* – (International) **Face authentication systems can be bypassed using a VR headset & Facebook photos.** Researchers from the University of North Carolina at Chapel Hill reported hackers could bypass face authentication systems on

the 1U App, BioID, KeyLemon, Mobius, and True Key after finding that if an attacker passes a high-resolution photo through a three-dimensional (3D) modeling software, then transfers the 3D head to a virtual reality (VR) device, a machine running the facial recognition software will authenticate the attacker. Researchers found that in photos where the quality was lower, such as social media photos, the authentication rate was lower.
Source: http://news.softpedia.com/news/face-authentication-systems-can-be-bypassed-using-a-vr-headset-facebook-photos-507568.shtml

For additional stories, see items **7** and **21**

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

20. *August 24, Help Net Security* – (International) **Cybercriminals select insiders to attack telecom providers.** Kaspersky Lab and B2B International researchers reported that 28 percent of all cyber-attacks involve malicious activity by insiders after finding that cybercriminals were using insiders to gain access to telecommunications networks and subscriber data, and recruiting employees through underground message boards, or through blackmail, forcing the employee to distribute spear-phishing campaigns on behalf of the attacker, hand over corporate credentials, or provide information on the company's internal systems in order to hack a targeted telecommunications firm.
Source: https://www.helpnetsecurity.com/2016/08/24/attack-telecom-providers/

21. *August 24, Softpedia* – (International) **Critical flaws let attackers hijack cellular phone towers.** Security researchers from Zimperium discovered three critical flaws affecting software packages from Legba Incorporated, Range Networks, and OsmoCOM, among other vendors running on Base Transceiver Station (BTS) stations, including a flaw in a core BTS software service that exposes the device to external connections, which could allow an attacker to reach the BTS station's transceiver and take remote control of the BTS station, extract information from the passing data, alter Global System for Mobile Communications (GSM) traffic, or crash the station. Researchers also discovered a memory buffer overflow bug that could allow an attacker to run malicious code on the device, and an issue that allows an attacker to remotely execute commands on the station's transceiver module without administrative credentials.
Source: http://news.softpedia.com/news/critical-flaws-let-attackers-hijack-cellular-phone-towers-507579.shtml

Commercial Facilities Sector

22. *August 24, Lower Hudson Valley Journal News* – (New York) **Smoking may have started Yonkers apartment fire.** A 3-alarm fire at a Yonkers, New York apartment complex August 24 displaced 17 families and injured 6 residents and 11 firefighters after the fire reportedly began when a resident fell asleep on a couch while smoking a cigarette. Authorities are investigating the exact cause of the fire.
Source: http://www.lohud.com/story/news/local/westchester/yonkers/2016/08/24/yonkers-fire/89248296/

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