Daily Open Source Infrastructure Report
11 July 2016

Top Stories

- A security researcher from Vulnerability Lab reported July 7 that BMW's ConnectDrive Web portal was plagued with two zero-day vulnerabilities including a cross-site scripting (XSS) flaw and a session vulnerability. – *Softpedia* (See item **4**)
- The chief of the Dallas Police Department announced July 8 that at least three gunman shot and killed five police officers and wounded seven others during a protest in Dallas July 7 over fatal police shootings in other States. – *Associated Press* (See item **16**)
- Senrio security researchers found that over 120 other D-Link products were plagued with the same remote-code execution (RCE) flaw found in the D-Link Network Cloud Cameras that could allow attackers to execute arbitrary code on the devices. – *Softpedia* (See item **19**)
- Wendy's fast food restaurant released an updated database July 7 which revealed that addition restaurant locations may have been affected by a 2015 security breach. – *United Press International; Wall Street Journal* (See item **22**)

Fast Jump Menu

Energy Sector

1. *July 8, U.S. Environmental Protection Agency* – (Colorado) **EPA announces stabilization work resuming at Gold King Mine.** The U.S. Environmental Protection Agency announced July 8 that contractors will begin work July 9 at the Gold King Mine in Colorado to complete work started during the fall of 2015 which will include stabilizing the mine adit and portal, continuing to operate the interim water treatment plant (IWTP) at Gladstone, and removing solids from retention ponds and filter bags, among other planned activities.
   Source: https://www.epa.gov/newsreleases/epa-announces-stabilization-work-resuming-gold-king-mine

2. *July 7, San Francisco Chronicle* – (California) **PG&E closes gas storage field in delta after finding leaks.** Pacific Gas and Electric Co., temporarily shut down its McDonald Island facility in the Sacramento-San Joaquin River Delta July 7, following the discovery of small leaks of flammable fuel. The company is investigating the source of the leaks and closed the facility out of an abundance of caution.
   Source: http://www.sfgate.com/business/article/PG-E-closes-gas-storage-field-in-Delta-after-8346829.php

Chemical Industry Sector

3. *July 7, Central Jersey Courier News* – (New Jersey) **Airborne leak contained at Edison chemical plant.** HAZMAT crews were deployed to Lyondell Industries in Edison after an equipment leak July 7 caused an airborne vapor to be released from the chemical facility. The leak was contained and officials confirmed there were no threats to public health.
   Source: http://www.mycentraljersey.com/story/news/crime/jersey-mayhem/2016/07/07/airborne-leak-contained-edison-chemical-plant/86808256/

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

4. *July 8, Softpedia* – (International) **Zero-days in BMW web portal let hackers tamper with customer cars.** A security researcher from Vulnerability Lab reported July 7 that BMW's ConnectDrive Web portal was plagued with two zero-day vulnerabilities including a cross-site scripting (XSS) flaw and a session vulnerability that can allow an attacker to bypass Vehicle Identification Number (VIN) session validation and use another car's VIN to access and edit another user's car settings. BMW has yet to patch the flaws.
   Source: http://news.softpedia.com/news/zero-days-in-bmw-web-portal-let-hackers-tamper-with-customer-cars-506103.shtml

5. *July 7, U.S. Department of Labor* – (Pennsylvania) **OSHA cites Amerway for again**

over exposing employees to lead hazards at Altoona manufacturing facility; failing to provide respiratory protection. The Occupational Safety and Health Administration cited Amerway Inc., with three repeat, four serious, and one other-than-serious violation July 1 after a March inspection at the Altoona, Pennsylvania facility revealed that the employer failed to implement engineering, administrative, and work practice controls to reduce employee exposure to lead, failed to institute a medical surveillance program, and failed to adequately label hazardous chemicals, among other violations. Proposed penalties total $49,000.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32781

6. *July 7, U.S. Consumer Product Safety Commission* – (National) **Kawasaki USA recalls recreational off-highway vehicles due to risk of injury.** Kawasaki Motors Corp., U.S.A. issued a recall July 7 for approximately 28,000 of its model years 2015 – 2017 Mule Pro side-by-side recreational off-highway vehicles sold in the U.S. due to an injury hazard where foreign objects can puncture the front floor board and strike operators and passengers. Kawasaki has received two reports in connection with the issue.
Source: http://www.cpsc.gov/en/Recalls/2016/Kawasaki-USA-Recalls-Recreational-Off-Highway-Vehicles/

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

7. *July 8, Huntsville Times* – (National) **Former Regions Bank VPs indicted in bribery, wire fraud scheme.** Two former vice presidents at Regions Bank, who also served as officers at Regions Equipment Financing Corp., (REFCO) in Birmingham, Alabama, were indicted July 7 for their roles in a $5 million bribery and wire fraud scheme where the duo and a co-conspirator allegedly established a fraudulent company, Residual Assurance Inc., that would enter an agreement with REFCO to provide residual value insurance, directed REFCO's residual value insurance business to the company, and split the business's proceeds between September 2010 and November 2015. The charges allege that the former executives collectively received over $3 million for their roles in the scheme.
Source:
http://www.al.com/news/index.ssf/2016/07/former_regions_bank_vps_indict.html

Transportation Systems Sector

8. *July 8, KETV 7 Omaha* – (Iowa) **Hazmat spill causes I-29 to close near Missouri Valley.** A single vehicle crash involving a semi-truck hauling 5,000 gallons of diesel additive, prompted the Iowa State Patrol to close Interstate 29 near Missouri Valley for nearly 2 hours July 7 while HAZMAT crews worked to clean the spill.

Source: http://www.ketv.com/news/hazmat-spill-causes-i29-to-close/40412992

9. *July 7, KTLA 5 Los Angeles* – (California) **'Hoax' device prompts closure of downtown L.A. Metro station, disruption of 4 Metro lines.** Officials closed the Seventh Street/Metro Center station in Los Angeles July 7 for nearly 3 hours after official found a suspicious unattended package in the station. The device was deemed a "hoax" and trains began their normal operations.
Source: http://ktla.com/2016/07/07/metro-center-station-closed-in-downtown-l-a-due-to-unattended-package/

10. *July 7, Rancho Santa Margarita Patch* – (California) **Tons of sand on Ortega Highway after semi vs. street sweeper accident.** State Route 74 in Rancho Santa Margarita was closed for more than 3 hour July 7 while crews worked to clear the wreckage from a two-vehicle accident involving an overturned truck that spilled 20,000 pounds of sand onto the highway after colliding with a street sweeper.
Source: http://patch.com/california/ranchosantamargarita/sig-alert-tons-sand-ortega-hwy-after-semi-vs-street-sweeper-accident

11. *July 7, KMVT 11 Twin Falls; KSVT 14 Twin Falls* – (Idaho) **State Highway 75 in Blaine County opens up after two-car collision.** Officials are investigating July 7 a head-on collision after the accident closed State Highway 75 in Hailey, Idaho for 2 hours and injured two people July 6.
Source: http://www.kmvt.com/content/news/Vehic-385777731.html

12. *July 7, Rhinelander Star Journal* – (Wisconsin) **A three-car collision in Oneida County leaves one person seriously injured.** Highway 47 in Oneida County was closed for several hours July 7 while crews worked to clear the wreckage from a three-vehicle crash that sent one driver to the hospital.
Source: http://www.starjournalnow.com/2016/07/07/a-three-car-collision-in-oneida-county-leaves-one-person-seriously-injured/

Food and Agriculture Sector

See item **17**

Water and Wastewater Systems Sector

13. *July 7, Denver Post* – (Colorado) **E. coli closes swim beach at state park in western Colorado.** Water officials temporarily closed the swim beach at Crawford State Park in western Colorado July 7 after officials detected elevated E. coli bacteria in the water when conducting weekly tests.
Source: http://www.denverpost.com/2016/07/07/e-coli-closes-swim-beach-at-state-park-in-western-colorado/

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

14. *July 7, Palm Desert Patch; California Department of Forestry and Fire Protection* – (California) **Calif. wildfire status report: Containment growing on many fires, but increased risk ahead, Cal Fire says.** More than 3,600 California firefighters worked July 7 to contain at least 10 wildfires that have collectively burned over 74,000 acres across the State.
Source: http://patch.com/california/palmdesert/calif-wildfire-status-report-containment-growing-many-fires-increased-risk

15. *July 7, Salt Lake Tribune* – (Utah) **Saddle Wildfire: Some growth, but 100 percent containment still expected July 15.** Crews reached 42 percent containment July 7 of the 1,939-acre Saddle Fire burning near St. George in the Dixie National Forest. Authorities expect to reach full containment by July 15, while voluntary evacuations and campground and hiking trail closures remain in effect.
Source: http://www.sltrib.com/news/4091297-155/saddle-wildfire-some-growth-but-100

Emergency Services Sector

16. *July 8, Associated Press* – (Texas) **Police: 5 officers dead, 7 hurt in Dallas protest shooting.** The chief of the Dallas Police Department announced July 8 that at least three gunman shot and killed five police officers and wounded seven others during a protest in Dallas July 7 over fatal police shootings in other States. One suspect was killed in an exchange with police and authorities were continuing to investigate the incident while searching for other suspects involved in the shootings.
Source: http://www.msn.com/en-us/news/breakingnews/police-5-officers-dead-7-hurt-in-dallas-protest-shooting/ar-BBu5aky?li=BBnb7Kz

17. *July 8, Associated Press* – (New York) **Officials: Salmonella outbreak in May at Suffolk jail.** Health officials reported July 8 that at least 21 inmates at the Suffolk County jail on Long Island were sickened in a Salmonella outbreak that began May 10 due to undercooked chicken that was served at the jail.
Source: http://www.centredaily.com/news/business/health-care/article88385852.html

Information Technology Sector

18. *July 7, Softpedia* – (International) **New "Patchwork" cyber-espionage group uses copy-pasted malware for its attacks.** Security researchers from Cymmetria reported that a new cyber-espionage group dubbed, Patchwork Advanced Persistent Threat (APT) was seen infecting at least 2,500 machines since December 2015 and can infect an underlying operating system (OS) with their malware using spear-phishing emails that contain PowerPoint files as attachments, which are embedded with the Sandworm exploit. The cyber criminals use an assortment of copy-pasted code from known malware such as PowerSploit, Meterpreter, Autolt, and UACME.
Source: http://news.softpedia.com/news/new-patchwork-cyber-espionage-group-uses-copy-pasted-malware-for-its-attacks-506101.shtml

For additional stories, see items **4** and **19**

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

19. *July 8, Softpedia* – (International) **D-Link vulnerability affects over 120 products, 400,000 devices.** Security researchers from Senrio discovered that over 120 other D-Link products were plagued with the same remote-code execution (RCE) vulnerability found in the D-Link DCS-930L Network Cloud Cameras that could allow attackers to execute arbitrary code on the devices. Researchers reported that an alleged 400,000 D-Link products could be affected.
Source: http://news.softpedia.com/news/d-link-vulnerability-affects-over-120-products-400-000-devices-506104.shtml

Commercial Facilities Sector

20. *July 8, WAVY 10 Portsmouth* – (Virginia) **Man admits to starting fire that gutted Va. Beach storage units.** The Oceana Self-Storage facility in Virginia Beach was destroyed and sustained more than $100,000 in damages July 7 due to an accidental blaze after a carburetor backfired and caught fire while a man was conducting repairs on his vehicle. The incident was contained and three firefighters were treated for heat exhaustion.
Source: http://wavy.com/2016/07/07/crews-working-fire-at-oceana-self-storage-in-va-beach/

21. *July 8, WLFI 18 West Lafayette* – (Indiana) **Fire officials: 'Apparent arson' in Logansport fires.** Closson Lumber & Peculiar Treasures in Logansport, Indiana, was deemed a total loss July 8 following a fire at the facility. Officials reported that the fire appears to be an act of arson and are investigating the incident.
Source: http://wlfi.com/2016/07/08/fire-consumes-more-than-100-year-old-logansport-family-business/

22. *July 7, United Press International; Wall Street Journal* – (National) **Wendy's says credit, debit card breach affected over a thousand U.S. locations.** Wendy's restaurant released an updated database July 7 which revealed that addition restaurant locations may have been affected by a 2015 security breach after the company discovered malware on the company's point-of-sale (PoS) systems May 2016. Company officials allegedly believe more than 1,000 nationwide locations were affected.
Source: http://www.upi.com/Business_News/2016/07/07/Wendys-says-credit-debit-

card-breach-affected-over-a-thousand-US-locations/5831467931159/

Dams Sector

23. *July 6, U.S. Army Corps of Engineers* – (Mississippi) **Repair work begins on Red River's Lindy C. Boggs Lock and Dam.** The U.S. Army Corps of Engineers announced July 6 that they would begin repair work on the Lindy C. Boggs Lock and Dam, located on the Red River, due to failed or failing connections following deteriorated nuts and washers that secure the hoist cable. Officials reported that the project will fix 5 of its 11 gates.
Source: http://www.mvk.usace.army.mil/Media/News-Releases/Article/827774/repair-work-begins-on-red-rivers-lindy-c-boggs-lock-and-dam/

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