Daily Open Source Infrastructure Report
19 April 2016

Top Stories

- General Motors Company issued a recall April 15 for nearly 895,232 Chevrolet Silverado and GMC Sierra 1500 pickups trucks after warranty data revealed that the steel cable which connects the seat belt to the vehicle can separate over time. – *Reuters* (See item **3**)
- Flooding across Houston April 18 prompted the closure of Interstate 10, the closure of 9 area hospitals, the evacuation of 3 apartment buildings, and the cancellation of 140 flights at the Hobby Airport. – *CNN* (See item **6**)
- Severe storms moving through southern Colorado April 15 prompted the closure of several highways as well as the cancellation of 845 flights at Denver International Airport April 15 – April 16. – *KRDO 13 Colorado Springs* (See item **7**)
- Cisco Talos security researchers discovered that 3.2 million computers were vulnerable to file-encrypting ransomware due to out-of-date software in government organizations, schools entities, and other organizations. – *SecurityWeek* (See item **15**)

Fast Jump Menu

Energy Sector

1. *April 15, Terre Haute Tribune-Star* – (Indiana) **Duke Energy shuts down coal-fired plant.** Duke Energy announced April 15 that decommissioning efforts were underway after units 2, 3, 4, and 5 of its Wabash River Generating Station in Indiana were shut down the week of April 4 as part of a 2013 settlement.
   Source: http://www.journalgazette.net/news/local/indiana/Duke-Energy-shuts-down-coal-fired-plant-12568614

For another story, see item **6**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

2. *April 17, WREX 13 Rockford* – (Illinois) **Belvidere Fiat Chrysler plant to shut down for one week.** Fiat Chrysler announced April 17 that its Belvidere, Illinois plant will be idle with no production during the week of April 18 due to an imbalance in supply and demand. The company reported that it will continue to monitor the market while the plant is temporarily shut down.
   Source: http://www.wrex.com/story/31744480/2016/04/17/belvidere-fiat-chrysler-plant-to-shut-down-for-one-week

3. *April 15, Reuters* – (International) **GM recalls 1 million trucks for faulty seat belts.** General Motors Company issued a recall April 15 for 895,232 model years 2014 – 2015 Chevrolet Silverado and GMC Sierra 1500 pickups, and a stop-sale of approximately 3,000 new pickups on dealer lots due to a seat belt flaw after warranty data showed that the flexible steel cable that connects the seat belt to the vehicle can separate over time as a result of the driver repeatedly bending the cable when entering the seat. The recall includes about 142,000 vehicles outside of the U.S.
   Source: http://www.cnbc.com/2016/04/15/gm-recalls-1-million-trucks-for-faulty-seat-belts.html

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *April 17, Santa Clarita Valley Signal* – (California) **Valencia man pleads guilty to fraud in $20 million precious metal investment scam.** The U.S. Attorney's Office

charged the owner of Superior Gold Group, LLC., and Superior Equity Group, LLC., for 4 counts of wire fraud, 5 counts of wire fraud, and 2 counts of money laundering as a part of a $20 million metal investment scam April 15 after the man defrauded more than 300 investors by failing to disclose material information to investors pertaining to the delivery of precious metals and cost investors to lose nearly $11 million while the man used the investors' money for personal expenditures from October 2007 – December 2010.
Source: http://www.signalscv.com/section/36/article/151166/

5. *April 15, U.S. Securities and Exchange Commission* – (California) **SEC charges litigation marketing company with bilking retirees.** The U.S. Security and Exchange Commission charged Los Angeles-based Prometheus Law and its two co-founders with conducting a Ponzi-like scheme April 15 after the duo raised $11.7 million from about 250 investors and retirees, promising investors that the funds would be allocated for marketing and advertising purposes to locate plaintiffs for class-action lawsuits, but instead the two diverted about $5.6 million for their personal use while failing to deliver the promised 100 to 300 percent returns to investors.
Source: https://www.sec.gov/news/pressrelease/2016-72.html

Transportation Systems Sector

6. *April 18, CNN* – (Texas) **Houston largely shut down amid rain, flooding.** Flooding in low-lying areas across Houston April 18 prompted the suspension of bus and rail service and the closure of portions of Interstate 10, schools, government offices, and 9 hospitals in the region. Three apartment buildings were evacuated, over 100,000 homes and businesses lost power, and 140 flights were cancelled at the Hobby Airport.
Source: http://www.cnn.com/2016/04/18/us/houston-texas-flooding/index.html

7. *April 17, KRDO 13 Colorado Springs* – (Colorado) **Highways closed, flights cancelled as spring storm pummels Colorado.** Severe storms that moved through southern Colorado April 15 prompted the closure of portions of Highway 24, Highway 94, and Highway 67, in addition to the cancellation of 845 flights at Denver International Airport April 15 – April 16.
Source: http://www.krdo.com/news/tornado-warning-issued-for-bent-and-kiowa-counties/39049534

8. *April 15, KNTV 11 San Jose* – (California) **Big rig carrying wine coolers flips on I-880 in Hayward, ties up traffic for 7 hours.** Highway 880 in Hayward was closed for approximately 7 hours April 15 due to a multi-vehicle accident involving three vehicles and a semi-truck carry a load of wine and wine coolers that jackknifed.
Source: http://www.nbcbayarea.com/news/local/Big-Rig-Carrying-Wine-Flips-on-I-880-in-Hayward-375834901.html

Food and Agriculture Sector

9. *April 18, U.S. Food and Drug Administration* – (National) **Advancepierre Foods recalls pork products due to misbranding and undeclared allergen.** AdvancePierre

Foods issued a recall April 16 for approximately 3,469 pounds of its CN Fully Cooked Breaded Pork Patties products packaged in 19.36-pound bags due to misbranding and undeclared egg which the company discovered during a routine labeling review. The products were shipped to establishments in Illinois, Kentucky, Ohio, and Iowa.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-030-2016-release

10. *April 15, U.S. Food and Drug Administration* – (Ohio; Indiana; Illinois) **Thomas Star Bakery of Ohio LLC issues voluntary recall on Buns Bread.** Thomas Star Bakery of Ohio LLC issued a voluntary recall April 14 for its Buns Bread products due to misbranding and undeclared milk and eggs, which was discovered during an Ohio Department of Agriculture inspection. The products were distributed to retail locations in Ohio, Indiana, and Illinois.
Source: http://www.fda.gov/Safety/Recalls/ucm496440.htm

11. *April 15, U.S. Food and Drug Administration* – (New York) **A&S Food Trading Inc. issues alert on undeclared sulfites in Gorgeous Memory Daylily.** A&S Food Trading Inc., issued a recall for its Gorgeous Memory Daylily products packaged in 10.6-ounce clear plastic bags April 14 after routine sampling by health officials determined that the products contained undeclared sulfites. The products were distributed to retail stores in the New York City area.
Source: http://www.fda.gov/Safety/Recalls/ucm496436.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

12. *April 15, Denver Post* – (Colorado) **Vail Valley hospital says former therapist took patient records.** A spokesperson for Vail Valley Medical Center in Colorado reported April 15 that a former physical therapist copied and took the personal and health information of 3,118 patients on two storage devices in December 2015. The medical center discovered the removal of patient information February 16 and upgraded its systems to restrict employees from moving or copying patient files.
Source: http://www.denverpost.com/news/ci_29772995/vail-valley-hospital-says-former-therapist-took-patient

Government Facilities Sector

13. *April 15, WXXI 1370 AM Rochester* – (New York) **Number of students with norovirus symptoms rises at the University of Rochester.** University of Rochester officials reported April 15 that the total number of students with norovirus-like symptoms increased to 116, and that the university will undergo extensive sanitization to address the outbreak over the weekend of April 16. University officials are working with the Monroe County Health Department to identify the source of the outbreak.
Source: http://wxxinews.org/post/number-students-norovirus-symptoms-rises-

university-rochester

14. *April 14, Berkshire Eagle* – (Massachusetts) **Flu outbreak closes Williamstown Elementary School for remainder of week.** Health officials ordered the shutdown of Williamstown Elementary School in Massachusetts April 13 – April 18 while crews thoroughly cleaned the building after more than 100 students and 20 staff members were reportedly sickened with the flu.
Source: http://www.berkshireeagle.com/local/ci_29763323/williamstown-elementary-school-shut-rest-week-due-flu

For additional stories, see items **6** and **15**

Emergency Services Sector

Nothing to report

Information Technology Sector

15. *April 18, SecurityWeek* – (International) **3.2 million devices exposed to ransomware attacks: Cisco.** Security researchers from Cisco Talos discovered that approximately 3.2 million computers were vulnerable to file-encrypting ransomware due to out-of-date software after an Internet scan on already compromised devices revealed that more than 2,100 backdoors across 1,600 Internet Protocol (IP) addresses were associated with governments, schools, aviation companies, and other organizations. Cisco advised administrators to disable external access to infected machine to keep attackers away.
Source: http://www.securityweek.com/32-million-devices-exposed-ransomware-attacks-cisco

16. *April 18, SecurityWeek* – (International) **C99 webshell increasingly used in WordPress attacks.** IBM Security reported that there was a 45 percent increase in attacks using a variant of the PHP webshell dubbed, C99 in WordPress Web sites after IBM identified nearly 1,000 attacks in February and March.
Source: http://www.securityweek.com/c99-webshell-increasingly-used-wordpress-attacks

17. *April 18, SecurityWeek* – (International) **Flaws found in Accuenergy, Ecava ICS products.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) released advisories detailing several flaws in its ICS products from Accuenergy Corporation, Ecava, and Sierra Wireless Company including an authentication bypass issue in Acuvim II and Acuvim IIR products, a security issue in Accuenergy devices, and an information disclosure vulnerability in Sierra's Wireless ACEmanager product, among other vulnerabilities.
Source: http://www.securityweek.com/flaws-found-accuenergy-ecava-ics-products

18. *April 17, Softpedia* – (International) **New USB-C standard can help fight USB malware.** The USB Implementers Forum (USB-IF) reported that it created a new standard titled, USB Type-C Authentication that will help protect USB-C capable

devise from low-end USB chargers that may inflict damage to a user's device and will help prevent USB malwares from infecting a device as the USB-C Authentication only sends data to a device that adheres to the strict USB-C specifications.
Source: http://news.softpedia.com/news/new-usb-c-standard-can-help-fight-usb-malware-503087.shtml

19. *April 16, Softpedia* – (International) **Decrypter available for AutoLocky, Locky ransomware copycat.** A security researcher from Emsisoft developed a decrytper for a new ransomware named AutoLocky, a variant of the Locky ransomware, which can encrypt a victim's file by tricking a victim into accessing a malicious link created inside the Start Menu StartUp folder named "Start.Ink." The decrypter was discovered after researchers found a flaw in the ransomware.
Source: http://news.softpedia.com/news/decrypter-available-for-autolocky-locky-ransomware-copycat-503053.shtml

20. *April 16, Softpedia* – (International) **Researcher identifies XSS filter bypass in Microsoft Edge.** A security researcher form PortSwigger discovered a bypass flaw in Microsoft's Edge's built-in cross-site scripting (XSS) filter that could allow attackers to run malicious JavaScript code inside its Edge Web browser while exploring several Web sites. Microsoft released a proof-of-concept code to users and reported a similar issue was seen in its Internet Explorer Web browser.
Source: http://news.softpedia.com/news/researcher-identifies-xss-filter-bypass-in-microsoft-edge-503054.shtml

21. *April 15, SecurityWeek* – (International) **VMware patches critical vulnerability.** VMware released updates for several of its products including a patch for a critical vulnerability in its Client Integration Plugin (CIP) that could have allowed an attacker to execute a man-in-the-middle (MitM) attack or session hijacking attack by tricking a vSphere Web client user to visit a specially crafted Web site. VMware advised its customers to update all programs to patch the flaw.
Source: http://www.securityweek.com/vmware-patches-critical-vulnerability

22. *April 15, SecurityWeek* – (International) **Western Digital user data exposed by DNS issue.** A security researcher discovered that a Western Digital (WD) nameserver, supporting the company's My Cloud NAS products, was not configured properly and posed a Domain Name System (DNS) flaw that could have been exploited by an attacker to conduct a zone transfer and gain access to a zone file, which can contain valuable user data for attackers to exploit a zero-day vulnerability in the products. WD corrected the faulty configuration after scanning all its servers and reviewing all the architecture and processes in place for modifying the configuration of nameservers.
Source: http://www.securityweek.com/western-digital-user-data-exposed-dns-issue

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

Nothing to report

Commercial Facilities Sector

23. *April 17, WPVI 6 Philadelphia* – (Pennsylvania) **3 injured in 3-alarm blaze at apartment complex in Pine Hill, N.J.** A 3-alarm fire at the Mansion Apartments in Pine Hill, New Jersey, injured 3 people, displaced 24 residents, and destroyed 8 apartment units April 16. One hundred firefighters contained the incident and the cause of the blaze was undetermined.
Source: http://6abc.com/news/3-injured-in-3-alarm-blaze-at-nj-apartment-complex-/1295198/

24. *April 15, WTVR 6 Richmond* – (Virginia) **Evacuation at Henrico shopping center lifted after robbery, suspicious package found.** The Laburnum Square Shopping Center in Henrico County, Virginia, was evacuated for nearly three hours April 15 while police and bomb squads investigated a suspicious package after a suspect robbed Check into Cash and left a suspicious package on the teller's counter. The package was removed and deemed safe.
Source: http://wtvr.com/2016/04/15/robbery-and-suspicious-package-situation/

For another story, see item **6**

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