Daily Open Source Infrastructure Report
17 August 2016

Top Stories

- Officials issued a safety order August 15 directing Washington Metropolitan Area Transit Authority (WMATA) to make changes to enhance safety after WMATA committed a total of 68 red signal violations since 2012. – *WTOP 103.5 FM Washington, D.C.* (See item **7**)
- The governor of Louisiana declared a state of emergency in East Baton Rouge, Louisiana, August 15 following severe storms August 12 – August 14 that left at least 4 people dead and displaced more than 10,000 residents. – *NBC News* (See item **10**)
- Officials reported August 15 that 13,237 patients at Professional Dermatology Care, P.C. in Reston, Virginia, were notified of a data breach after hackers may have gained access to protected patient information from the provider's network server between June 19 and June 27. – *Reston Patch; U.S. Department of Health and Human Services* (See item **11**)
- Lookout researchers reported that 1.4 billion Android devices are affected by a security flaw in the Linux kernel's implementation of the Transmission Control Protocol (TCP) that could allow a hacker to hijack unencrypted Web traffic. – *Softpedia* (See item **19**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

1. *August 15, Platts* – (Connecticut) **Dominion's Millstone-2 nuclear unit at 100% capacity after maintenance outage.** Dominion's Millstone-2 nuclear reactor at its Millstone Nuclear Power Plant in Waterford, Connecticut, returned to full operating capacity August 15 following a 2-day maintenance outage the weekend of August 13 to replace uninterruptible power supplies after a severe lightning storm affected the electrical supply to 2 of the 4 circulating water pumps and the power supplies failed to function as designed. The Millstone-3 nuclear reactor was not affected by the shutdown and continued operating at full capacity during the maintenance.
Source: http://www.platts.com/latest-news/electric-power/washington/dominions-millstone-2-nuclear-unit-at-100-capacity-21253322

Critical Manufacturing Sector

2. *August 15, SecurityWeek* – (International) **Flaw allows attackers to modify firmware on Rockwell PLCs.** Cisco Talos researchers discovered a high severity flaw in Rockwell Automation, Inc.'s Allen Bradley MicroLogix 1400 programmable logic controllers (PLCs) where an undocumented Simple Network Management Protocol (SNMP) community string, dubbed "wheel" could be exploited to make unauthorized changes to a device, including replacing the original firmware with a malicious version. Rockwell Automation advised customers to use the RUN key switch setting to prevent unauthorized firmware updates and configuration changes.
Source: http://www.securityweek.com/flaw-allows-attackers-modify-firmware-rockwell-plcs

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *August 15, KRON 4 San Francisco* – (California) **'Bearded Bandit' bank robbery suspect arrested in San Francisco.** FBI officials reported August 15 that a man dubbed the "Dreaded Bandit" was arrested in San Francisco August 12 after he allegedly committed 4 bank robberies in the San Francisco Bay Area since April.
Source: http://kron4.com/2016/08/15/bearded-bandit-bank-robbery-suspect-arrested-in-san-francisco/

For another story, see item **20**

Transportation Systems Sector

4. *August 16, WHTM 27 Harrisburg*– (Pennsylvania) **I-283 SB back open after tractor trailer carrying cattle overturns.** Southbound lanes of Interstate 283 in Harrisburg, Pennsylvania, were closed for nearly 5 hours August 16 while crews worked to clear the road after a semi-truck carrying 110 cows overturned onto the Interstate 283 east ramp, setting 9 cows loose and leaving more than 50 dead.
   Source: http://abc27.com/2016/08/15/overturned-tractor-trailer-carrying-cattle-causes-closure-on-i-283-sb/

5. *August 15, WRC 4 Washington, D.C.* – (Washington, D.C.) **5-year-old girl killed in violent crash along I-66W in Haymarket.** A 4-vehicle crash closed westbound lanes of Interstate 66 in Haymarket, Virginia, for nearly 4 hours August 15. One person was killed and two others were sent to an area hospital with serious injuries.
   Source: http://www.nbcwashington.com/news/local/Serious-Crash-Blocks-I-66-West-in-Haymarket-390182781.html

6. *August 15, Glenwood Springs Post Independent/Rifle Citizen Telegram* – (Colorado) **Two killed in Saturday accident on U.S. 6.** A single-vehicle crash left 2 people dead and prompted the closure of U.S. Route 6 between Canyon Creek and New Castle, Colorado for about 4 hours August 13 while Colorado State Patrol investigated the scene of the crash.
   Source: http://www.postindependent.com/news/local/two-killed-in-saturday-accident-on-u-s-6/

7. *August 15, WTOP 103.5 FM Washington, D.C.* – (Washington, D.C.) **After series of close calls, Metro ordered to make urgent fixes.** The Federal Transit Administration issued a safety order August 15 directing Washington Metropolitan Area Transit Authority (WMATA) to make 11 changes to enhance rider and worker safety following an investigation that found that WMATA committed a total of 68 confirmed red signal violations from January 2012 – July 2016, among other violations. The 11 corrective actions require WMATA to increase oversight of train operator and controllers, review its fatigue management system, and consider new options to automatically stop trains before collisions.
   Source: http://wtop.com/tracking-metro-24-7/2016/08/series-trains-blow-red-signals-metro-ordered-make-urgent-fixes/

For another story, see item **10**

Food and Agriculture Sector

8. *August 16, KHON 2 Honolulu* – (Hawaii) **Hepatitis A source served at Genki Sushi; Oahu, Kauai restaurants closed immediately.** Hawaii State Department of Health officials ordered all Genki Sushi restaurants on Oahu and Kauai to close August 15 after a hepatitis A outbreak that has sickened 168 people across the State was

potentially linked to imported frozen scallops served raw at the restaurant's Oahu and Kauai locations. Officials were working to identify the source of the tainted scallops.
Source:
http://khon2.com/2016/08/15/hepatitis-a-source-determined-to-be-genki-sushi-oahu-kauai-restaurants-closed-immediately/

For another story, see item **4**

Water and Wastewater Systems Sector

9. *August 15, Associated Press* – (Kansas) **Manhattan residents urged to boil water after a power outage.** The Kansas Department of Health and Environment issued a boil water advisory for Manhattan, Kansas residents August 15 following a power outage that led to a loss of pressure, creating the potential for bacterial contamination in the public water supply.
Source: http://www2.ljworld.com/news/2016/aug/15/manhattan-residents-urged-boil-water-after-power-o/

10. *August 15, NBC News* – (Louisiana) **Louisiana flooding: At least four dead, 20,000 rescued.** The governor of Louisiana declared a state of emergency in East Baton Rouge, Louisiana, August 15 following severe storms August 12 – August 14 that left at least 4 people dead, forced the closure of more than 100 roads across the State, damaged thousands of homes, and forced more than 10,000 residents to move to shelters August 14. Officials stated that over 1,700 rescue personnel saved more than 20,000 people from the flooding.
Source: http://www.nbcnews.com/news/us-news/louisiana-flooding-least-three-dead-officials-warn-more-rain-come-n630331

Healthcare and Public Health Sector

11. *August 15, Reston Patch; U.S. Department of Health and Human Services* – (Virginia) **Reston doctor's office hacked, 13,000 patient records compromised.** U.S. Department of Health and Human Services officials reported August 15 that 13,237 patients at Professional Dermatology Care, P.C. in Reston, Virginia, were notified of a data breach after hackers outside of the U.S. may have gained unauthorized access to protected patient information and financial data, including patient names, Social Security numbers, and Medicare numbers, among other information, from the provider's network server between June 19 and June 27 with the intent to extract money from the company in order to de-encrypt data. The company does not believe the hackers misused any of the patient data.
Source:
http://patch.com/virginia/reston/reston-doctors-office-hacked-13-000-patient-records-compromised

12. *August 15, U.S. Food and Drug Administration*– (International) **Cook Medical issues global recall of Roadrunner UniGlide Hydrophilic Wire Guides due to raw materials issue.** Cook Group Incorporated issued a recall August 15 for 8,750 units of

its Roadrunner Uniglide Hydrophilic Wire Guide products due to potential contamination with glass particles after the company's supplier, DSM Biomedical B.V., recalled certain lots of its hydrophilic coating used in the wire guide products due to potential glass fragment contamination. No adverse reactions have been reported and the products were distributed internationally.
Source:
http://www.fda.gov/Safety/Recalls/ucm516701.htm

For another story, see item **8**

Government Facilities Sector

13. *August 15, WTTG 5 Washington, D.C.* – (Washington, D.C.) **Washington Monument reopens after weekend power problems.** The Washington Monument in Washington, D.C. reopened August 15 after a voltage drop of incoming power caused a breaker to trip, cutting power to the elevator and leaving visitors stranded August 14.
Source: http://www.fox5dc.com/news/191301075-story

14. *August 15, Austin American-Statesman* – (Texas) **Pickle building evacuated after electrical fire; workers sent home.** The J.J. Pickle Federal Building in Austin, Texas, was evacuated and closed until further notice August 15 after an electrical fire related to an underground streetlight cable sent smoke throughout the facility and affected traffic signals on San Jacinto Boulevard. Austin Energy officials were working to repair the traffic signals.
Source: http://www.statesman.com/news/news/local/pickle-building-evacuated-as-firefighters-tackle-e/nsGGx/

15. *August 14, Charleston Gazette-Mail* – (West Virginia) **AC, power failures close 4 Kanawha schools Monday.** The superintendent of the Kanawha County public school system announced August 14 that 4 of the county's schools would be closed until August 16 due to air conditioning and power failures. Seven of the county's schools were closed August 12 due to similar issues.
Source: http://www.wvgazettemail.com/news-advisories/20160814/ac-power-failures-close-4-kanawha-schools-monday

Emergency Services Sector

16. *August 15, Manchester Patch* – (New Jersey) **Man stole $30K from Manchester Volunteer Fire Company: Police.** The former treasurer of the Manchester Volunteer Fire Company in Manchester, New Jersey, was charged August 15 after he allegedly embezzled over $30,000 from the department between 2012 and 2015 by writing checks to himself from the company's general account while serving as treasurer. Officials stated the former treasurer used the stolen money for personal expenses.
Source: http://patch.com/new-jersey/manchester-nj/man-stole-30k-manchester-volunteer-fire-company-police

Information Technology Sector

17. *August 16, Softpedia* – (International) **FalseCONNECT vulnerability affects software from Apple, Microsoft, Oracle, more.** A security researcher discovered a flaw in how applications from several vendors respond to Hypertext Transfer Protocol (HTTP) CONNECT requests via HTTP/1.0 407 Proxy Authentication Required responses which could allow an attacker with a foothold in a compromised network and the ability to listen to proxy traffic to detect HTTP CONNECT requests sent to the local proxy and issue a 407 Proxy Authentication Required response where the user must input a password to access a specific service and then authenticate, thereby sending the response to the malicious actor. Researchers stated that WebKit-based clients including Google Chrome, Apple's iTunes, and Google Drive, among others, are most vulnerable to the attack.
Source: http://news.softpedia.com/news/falseconnect-vulnerability-affects-software-from-apple-microsoft-oracle-more-507329.shtml

18. *August 15, SecurityWeek* – (International) **Windows script files used to deliver Locky ransomware.** Researchers from Trend Micro warned that a Locky ransomware variant was being delivered to targeted organizations using Microsoft Windows script (WSF) files in order to download any malware payload and to make detection more difficult, as WSF files are not engine-specific, contain more than one scripting language, and are not monitored by typical endpoint security solutions, thereby increasing the chances of bypassing sandboxes and blacklisting technologies. Researchers stated the cybercriminals were targeting companies and that the files delivering Locky were compressed in ZIP archives and attached to emails with business-related subject lines.
Source: http://www.securityweek.com/windows-script-files-used-deliver-locky-ransomware

For additional stories, see items **2** 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. *August 15, Softpedia* – (International) **1.4 billion Android devices affected by Linux TCP flaw.** Lookout security researchers reported that a security flaw in the Linux kernel's implementation of the Transmission Control Protocol (TCP), which could allow a malicious actor to hijack unencrypted Web traffic or shutdown encrypted connections between two parties without a man-in-the-middle (MitM) position also affects 1.4 billion Android devices running versions 4.4 or higher, as the Android mobile operating system (OS) is built on a modified version of the Linux kernel. Researchers advised users to encrypt their traffic by employing a virtual private

network (VPN), among other methods, to protect their devices.
Source: http://news.softpedia.com/news/1-4-billion-android-devices-affected-by-linux-tcp-flaw-507317.shtml

Commercial Facilities Sector

20. *August 15, SecurityWeek; Forbes* – (International) **MICROS hackers targeted five other PoS vendors.** Cybercrime monitoring company Hold Security reported that the hackers responsible for installing malicious code on select Oracle Corporation legacy MICROS point-of-sale (PoS) systems also potentially breached the systems of five other PoS vendors, including ECRS, Cin7, PAR Technology, Navy Zebra, and Uniwell. Navy Zebra is investigating the possible breach, while Cin7, PAR Technology, Uniwell, and ECRS confirmed detection of malicious code on their Web portals and stated no sensitive information has been compromised.
Source: http://www.securityweek.com/micros-hackers-targeted-five-other-pos-vendors

21. *August 15, Lower Hudson Valley Journal News* – (New York) **Yonkers fire displaces nearly 90 people.** A 4-alarm fire August 15 at a Yonkers, New York apartment complex left 89 residents displaced and several firefighters injured. The American Red Cross was assisting those displaced by the fire.
Source:
http://www.lohud.com/story/news/local/westchester/yonkers/2016/08/15/yonkers-fire-displaces-dozens/88758190/

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

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.