Daily Open Source Infrastructure Report
19 August 2016

Top Stories

- Authorities are searching August 17 for a group suspected of stealing tens of thousands of dollars from more than 100 people in St. Paul, Minnesota, after installing skimming devices on 2 ATMs at area banks. – *KARE 11 Minneapolis* (See item **3**)
- A Miami resident pleaded guilty August 15 for his role in a $4.2 million health care fraud scheme where he facilitated the submission of fraudulent claims to Medicare beginning in March 2014. – *U.S. Department of Justice* (See item **12**)
- Cisco released security patches after The Shadow Brokers, a group selling stolen hacking tools, leaked tools that contain exploits to leverage a zero-day vulnerability in the Simple Network Management Protocol (SNMP) code of Cisco Adaptive Security Appliance (ASA) software, which can lead to remote code execution. – *Softpedia* (See item **17**)
- The governor of Pennsylvania issued $25.7 million in funding August 17 for repairs at 5 high-hazard damns in the State, including Donegal Lake in Westmoreland County and Somerset Lake in Somerset County. – *Pittsburg Tribune-Review* (See item **23**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

1. *August 16, Quincy Patriot Ledger* – (Massachusetts) **Pilgrim nuclear plant at half power for maintenance.** Entergy Corporation reduced power at its Pilgrim Nuclear Generating Station in Plymouth, Massachusetts, to 47 percent August 16 while crews completed scheduled maintenance, including a thermal backwash. Officials did not disclose when the plant would return to full operating power.
Source: http://www.wickedlocal.com/news/20160816/pilgrim-nuclear-plant-at-half-power-for-maintenance

Critical Manufacturing Sector

2. *August 17, U.S. Department of Labor* – (New Jersey) **National Manufacturing Co. exposes workers to chemical hazards, workplace safety dangers at north Jersey facility.** The Occupational Safety and Health Administration cited National Manufacturing Co. Inc. with 10 serious safety violations July 25 following a January 2016 incident where a worker was burned in a flash fire while cleaning a degreasing tank, prompting an investigation at the Chatham, New Jersey facility, which revealed that the company failed to provide fall protection for workers, failed to protect employees from hazards related to N-Propyl Bromide, and failed to prevent electrical and housekeeping hazards, among other violations. Proposed penalties total $56,300.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=33012

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *August 17, KARE 11 Minneapolis* – (Minnesota) **Thousands stolen with ATM skimmers in St. Paul.** Authorities are searching August 17 for a group suspected of stealing tens of thousands of dollars from more than 100 people in St. Paul, Minnesota, after installing skimming devices on 2 ATMs at a Bremer Bank branch and a Top Line Federal Credit Union branch in St. Paul.
Source: http://www.kare11.com/news/suspects-stealing-atm-card-information/300877065

Transportation Systems Sector

4. *August 18, Raleigh News & Observer* – (North Carolina) **Motorcycle-pickup crash in Durham kills rider.** Highway 55 in Durham, North Carolina, was closed for several hours August 17 while authorities investigated the cause of an accident where a motorcycle crashed into another vehicle, killing the motorcyclist.
Source: http://www.newsobserver.com/news/traffic/article96358222.html

5. *August 18, WKYC 3 Cleveland* – (Ohio) **Man dies when Focus crashes head-on with semi.** U.S. 250 in Ashland, Ohio, was closed for more than 4 hours August 18 while crews worked to clear the wreckage after a vehicle crossed the center line and struck a semi-truck head-on, killing one person and injuring another. The cause of the crash remains under investigation.
Source: http://www.wkyc.com/traffic/man-dies-when-focus-crashes-head-on-with-semi/301530069

6. *August 18, Washington Post* – (Maryland) **Part of Indian Head Highway reopens after serious crash.** Northbound lanes of Indian Head Highway in Fort Washington, Maryland, were closed for nearly 4 hours August 18 while Prince George's County officials investigated the scene after a pedestrian was struck by a vehicle. The pedestrian was transported to an area hospital with critical injuries.
Source: https://www.washingtonpost.com/news/dr-gridlock/wp/2016/08/18/part-of-indian-head-highway-closed-after-serious-crash/

7. *August 17, KEYT 3 Santa Barbara/KCOY 12 Santa Maria/KKFX 24 San Luis Obispo* – (California) **Highway 1 closed near Lompoc after big rig crash.** Highway 1 between U.S. Highway 101 and Highway 246 in Lompoc, California, was closed for several hours August 17 while officials investigated the scene after a semi-truck traveling northbound crossed the center line and struck 2 other semi-trucks. Officials reported the same portion of Highway 1 would be closed August 18 for 12 hours while crews work to clean up a diesel spill caused by the collision.
Source: http://www.keyt.com/news/hwy-1-closed-near-lompoc-by-serious-accident/41248850

8. *August 17, Associated Press* – (Puerto Rico) **More than 500 evacuated in ship fire near Puerto Rico.** More than 500 passengers aboard American Cruise Ferries' Caribbean Fantasy cruise and ferry ship off the coast of Puerto Rico were evacuated from the ship August 17 after a hose carrying fuel burst open and caught fire. Officials reported that 24 passengers were transported to an area hospital with injuries.
Source: http://brooklyn.news12.com/news/more-than-500-evacuated-in-cruise-ship-fire-near-puerto-rico-1.12189864

9. *August 17, WRDW 12 Augusta/WAGT 26 Augusta* – (Georgia) **400 gallon diesel spill causes headaches along Mike Padgett.** Mike Padgett Highway in Richmond County, Georgia, was closed for nearly 3 hours August 17 while crews worked to clear 400 gallons of diesel that spilled after two semi-trucks collided.
Source: http://www.wrdw.com/content/news/Accident-involving-two-tractor-trailers-

on-Mike-Padgett-Hwy-at-4-H-Club-Rd-390440251.html

Food and Agriculture Sector

10. *August 17, U.S. Food and Drug Administration*– (California) **Bakers of Paris recalls croissants sold at Whole Foods Market stores in northern California due to undeclared allergen.** Bakers of Paris issued a recall August 16 for its plain and chocolate croissant products due to undeclared egg. One allergic reaction has been reported in connection with the products which were distributed to 18 Whole Foods Market Inc. stores in northern California.
Source:
http://www.fda.gov/Safety/Recalls/ucm517124.htm

Water and Wastewater Systems Sector

11. *August 18, Frederick News-Post* – (Maryland) **Over 15,000 gallons of raw sewage spilled in Brunswick.** Heavy rains in Brunswick, Maryland, August 17 caused more than 15,000 gallons of raw sewage to leak out of manholes in the Brunswick American Legion's parking lot on Maple Avenue and on Walnut Street. City officials advised the public to avoid contact with standing water in the area.
Source: http://www.fredericknewspost.com/news/disasters_and_accidents/over-gallons-of-raw-sewage-spilled-in-brunswick/article_b50de16b-8aae-5454-a86f-87182dfe4b9c.html

Healthcare and Public Health Sector

12. *August 15, U.S. Department of Justice* – (Florida) **Miami man pleads guilty to fraud charges for role in $4.2 million home health care scheme.** A Miami resident pleaded guilty August 15 for his role in a $4.2 million health care fraud scheme where he was recruited by the owners of Golden Home Health Care Inc. to falsely and fraudulently represent himself as an owner of the company, and signed Medicare applications and other documents in order to facilitate the submission of fraudulent claims to Medicare beginning in March 2014. Officials stated that two co-conspirators were charged for their roles in the scheme in June 2016.
Source:
https://www.justice.gov/opa/pr/miami-man-pleads-guilty-fraud-charges-role-42-million-home-health-care-scheme

Government Facilities Sector

13. *August 18, Santa Rosa Press Democrat* – (California) **Firefighters gain upper hand on Lake County's Clayton fire.** Officials lifted evacuation orders for 4,000 Clearlake, California residents August 16 after crews reached 35 percent containment of the 4,000-acre Clayton Fire burning in Lake County, which has destroyed at least 175 structures and threatens 380 homes. Evacuation orders remained in place for Lower Lake residents.
Source: http://www.pressdemocrat.com/news/5977765-181/progress-on-clayton-fire-

20?gallery=5979418&artslide=0

14. *August 17, Associated Press* – (Washington, D.C.) **Washington Monument closed again after elevator problems.** The U.S. National Park Service announced August 17 that the Washington Monument in Washington, D.C. will be closed until August 19 to make repairs after the elevator's compensating cable broke loose from the car, causing the elevator to stop operating.
Source: https://www.washingtonpost.com/politics/washington-monument-closed-again-after-elevator-problems/2016/08/17/659c4510-64ac-11e6-b4d8-33e931b5a26d_story.html

15. *August 17, WVIT 30 New Britain* – (Connecticut) **Lake Waramaug, Squantz Pond swimming areas closed.** Officials from the Connecticut Department of Energy and Environmental Protection (DEEP) closed the swimming areas at Lake Waramaug State Park in Kent and Squantz Pond State Park in New Fairfield August 17 after routine testing revealed high levels of bacteria that could indicate potential contamination in the water. DEEP officials were retesting the water to determine when the swimming areas will reopen.
Source: http://www.nbcconnecticut.com/news/local/Lake-Waramaug-Squantz-Pond-Swimming-Areas-Closed-390437451.html

Emergency Services Sector

Nothing to report

Information Technology Sector

16. *August 18, SecurityWeek* – (International) **Cisco patches critical flaws in Firepower Management Center.** Cisco released patches for its Firepower Management Center to address several flaws in the appliance's Web-based graphical user interface (GUI) including a medium-severity cross-site scripting (XSS) flaw, a critical vulnerability that could allow an authenticated attacker to remotely execute arbitrary commands on a device with root-level privileges, and a flaw that could allow an authenticated attacker to elevate user account privileges due to insufficient authorization checking in the Fire Management Center and the Cisco ASA 5500-X series with select versions of FirePOWER Services. Cisco researchers stated there is no evidence the flaws have been exploited in the wild.
Source: http://www.securityweek.com/cisco-patches-critical-flaws-firepower-management-center

17. *August 17, Softpedia* – (International) **Cisco patches zero-day included in Shadow Brokers leak.** Cisco released security patches after The Shadow Brokers, a group selling hacking tools stolen from the Equation Group, leaked tools that contain exploits to leverage two vulnerabilities, one of which is a zero-day vulnerability in the Simple Network Management Protocol (SNMP) code of Cisco Adaptive Security Appliance (ASA) software, which can allow an unauthenticated attacker to cause a reboot of affected products and lead to remote code execution (RCE). Cisco researchers found

that the exploits also leverage a vulnerability in the command-line interface (CLI) parse of ASA software that could allow an authenticated, local attacker to execute arbitrary code on the device or create a denial-of-service (DoS) condition.
Source: http://news.softpedia.com/news/cisco-patches-zero-day-exposed-in-shadow-brokers-leak-507410.shtml

18. *August 17, Softpedia* – (International) **WordPress plugin hijacks websites to show payday loan ads.** WordFence researchers discovered the authors of the 404 and 301 WordPress plugin were hijacking the content of other Web sites by adding code to the original Web site in order to show search engine optimization (SEO) spam email on a user's homepage and to display ads for payday loan services. The plugin authors removed the code responsible for delivering the ads and researchers stated version 2.3.0 is safe to use.
Source: http://news.softpedia.com/news/wordpress-plugin-hijacks-websites-to-show-payday-loan-ads-507402.shtml

19. *August 17, Softpedia* – (International) **Adwind RAT rebrands yet again, this time as JBifrost.** Fortinet researchers discovered that the criminal group behind the Adwind remote access trojan (RAT) rebranded the malware as JBifrost and updated the malware to include a new column that shows an infected system's keyboard status, a column that shows the title of the victim's current window, a new feature that enables attackers to steal data from Web forms displayed in the Google Chrome browser, and a new tab called Misc that enables users to configure additional JBifrost servers. Researchers also found that JBifrost only accepts Bitcoin and that the RAT's Web site now requires an invitation code to register and purchase the malware.
Source: http://news.softpedia.com/news/adwind-rat-rebrands-yet-again-this-time-as-jbifrost-507395.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

Communications Sector

Nothing to report

Commercial Facilities Sector

20. *August 18, KTRK 13 Houston* – (Texas) **No injuries in 3-alarm apartment fire in NW Harris Co.** A 3-alarm fire at the Yorktown Crossing Apartments in northwest Harris County, Texas, August 17 destroyed 26 units after the fire reportedly began when lightning struck the building. No injuries were reported.
Source: http://abc13.com/news/firefighters-respond-to-3-alarm-apartment-fire-in-nw-

harris-co/1474009/

21. *August 18, KXAS 5 Fort Worth* – (Texas) **Dallas high-rise apartments evacuated over carbon monoxide leak.** All residents were evacuated from the CityWalk Apartments in Dallas for several hours August 17 after a boiler malfunction in the basement caused a carbon monoxide leak. Crews shut off the boiler and ventilated the building before allowing residents to return inside.
Source: http://www.nbcdfw.com/news/local/Dallas-High-Rise-Apartments-Evacuated-Over-Possible-Gas-Leak-390522241.html

22. *August 16, NJ.com* – (New Jersey) **$300K in trucks, trailers, landscaping equipment stolen in Morris Plains.** Authorities are investigating August 16 after $300,000 worth of equipment, including commercial vehicles, enclosed trailers, and landscaping equipment, was stolen from an A-L Services Inc., company storage area in Morris Plains, New Jersey, August 13.
Source:
http://www.nj.com/morris/index.ssf/2016/08/300k_in_trucks_trailers_and_landscaping_equipment.html

Dams Sector

23. *August 17, Pittsburg Tribune-Review* – (Pennsylvania) **State releases $25.7M to repair unsafe dams at Donegal, Somerset lakes.** The governor of Pennsylvania issued $25.7 million in funding August 17 for repairs at 5 high-hazard dams in the State, including Donegal Lake in Westmoreland County and Somerset Lake in Somerset County, as well as 3 other dams. Officials stated the funding will also pay for the start of design work on dams in Belmont Lake and Lower Woods Pond in Wayne County.
Source: http://triblive.com/news/westmoreland/10985948-74/lake-dams-county

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