Homeland Security

Daily Open Source Infrastructure Report 21 July 2016

Top Stories

- Crews worked July 19 to restore power to about 69,800 customers in east Idaho, Wyoming, and Montana who remained without service after a capacitor bank caught fire at the Goshen substation near Shelley, Idaho. – *KPVI 6 Pocatello* (See item **2**)
- Bar-S Foods Company issued a recall July 19 for approximately 372,684 pounds of its chicken and pork hot dog and corn dog products sold in 5 variations due to potential Listeria monocytogenes contamination. – *U.S. Department of Agriculture* (See item **9**)
- Oracle released its July Critical Patch Update (CPU) that addressed a total of 276 vulnerabilities in several of its products including 36 security flaws in applications specifically designed for the insurance, health, financial, and utility sectors.– *SecurityWeek* (See item **15**)
- A former employee at White's Farm Supply, Inc., in Lenox, New York, was charged July 19 after he allegedly embezzled over $740,000 from the company since 2009. – *WTVH 5 Syracuse* (See item **23**)

Fast Jump Menu

PRODUCTION INDUSTRIES

- Energy
- Chemical
- Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH

- Food and Agriculture
- Water and Wastewater Systems
- Healthcare and Public Health

SERVICE INDUSTRIES

- Financial Services
- Transportation Systems
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE

- Government Facilities
- Emergency Services

Energy Sector

1. *July 20, WWBT 12 Richmond* – (Virginia) **More than 46,000 Dominion customers without power due to storms.** Dominion Virginia Power crews worked July 20 to restore power to more than 46,000 customers who remained without service after severe storms moved through the Richmond Metro area July 19 knocking out power to more than 71,000 customers.
Source: http://www.nbc12.com/story/32482215/more-than-50000-dominion-customers-without-power-due-to-storms

2. *July 20, KPVI 6 Pocatello* – (Idaho) **Massive power outage impacts three state region.** Crews worked July 19 to restore power to about 69,800 Idaho Falls Power, Rocky Mountain Power, Lower Valley Energy Inc., and Fall River Rural Electric Cooperative customers in east Idaho, Wyoming, and Montana who remained without service after a capacitor bank caught fire at the Goshen substation near Shelley, Idaho.
Source: http://www.kpvi.com/news/massive-power-outage-impacting-three-state-region/article_f6fe884c-4e09-11e6-b10b-734def26ad5a.html

3. *July 19, NBC News; FlightAware.com* – (National) **Severe Northeast storms leave one dead, knock out power for thousands.** Crews worked July 19 to restore power to more than 12,000 customers who remained without service after strong storms moved through Pennsylvania and northern New England July 18 knocking out power to over 100,000 customers and causing more than 300 flights from Newark Liberty International Airport in New Jersey, LaGuardia Airport in New York, and Logan International Airport in Massachusetts to be cancelled.
Source: http://www.nbcnews.com/news/weather/severe-northeast-storms-leave-one-dead-knock-out-power-thousands-n612286

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *July 19, Sacramento Bee* – (California, Nevada) **Man dubbed 'Bandaged Bandit'**

sought in area bank robberies. The FBI is searching for a man dubbed the "Bandaged Bandit" who is suspected of committing four bank robberies in El Dorado Hills, California, and in Folsom and Stateline, Nevada, since June, including a U.S. Bank branch in Folsom July 15.
Source: http://www.sacbee.com/news/local/crime/article90701467.html

For additional stories, see items **15** and **23**

Transportation Systems Sector

5. *July 20, NJ.com* – (New Jersey) **Route 22 open after serious motorcycle accident in Bridgewater.** Route 22 in Bridgewater, New Jersey, was closed for 3 hours July 20 following a two-vehicle accident involving a motorcycle and another vehicle that sent one person to an area hospital with injuries.
Source: http://www.nj.com/somerset/index.ssf/2016/07/serious_motorcycle_accident_on_route_22_in_bridgew.html

6. *July 20, WITI 6 Milwaukee* – (Wisconsin) **1 killed, 1 seriously hurt in head-on crash on I-94 in Delafield.** Interstate 94 in Delafield, Wisconsin, was closed for several hours July 19 while officials investigated the scene of a head-on crash that left one person dead and sent two others to area hospitals with injuries.
Source: http://fox6now.com/2016/07/19/traffic-alert-all-eastbound-lanes-of-i-94-at-wis-83-closed-due-to-crash/

7. *July 19, WBIR 10 Knoxville* – (Tennessee) **THP: Truck driver killed, 2 others hurt in I-75 crash.** Northbound lanes of Interstate 75 in Loudon County, Tennessee, were closed for about 3 hours July 19 while crews worked to clear the wreckage from a fatal two-vehicle crash after a semi-truck crashed into the median, overturned, and was struck by an oncoming vehicle. One person was killed and two others were injured.
Source: http://www.wbir.com/news/local/crash-shuts-down-i-75-in-loudon-co/276674327

For another story, see item **3**

Food and Agriculture Sector

8. *July 20, U.S. Food and Drug Administration* – (National) **Agave Dream recalls Cappuccino Ice Cream because of possible health risk.** Agave Dream, Inc., issued a recall July 19 for 389 cases of its Cappuccino Ice Cream products due to potential Listeria monocytogenes contamination after routine sampling revealed that the finished ice cream products contained Listeria. The company has ceased the production and distribution of the products and no illnesses were reported in connection with the products which were distributed to select retail stores nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm512109.htm

9. *July 20, U.S. Department of Agriculture* – (National) **Bar-S Foods Company recalls**

chicken and pork hot dog and corn dog products due to possible Listeria contamination. Bar-S Foods Company issued a recall July 19 for approximately 372,684 pounds of its chicken and pork hot dog and corn dog products sold in 5 variations due to potential Listeria monocytogenes contamination after recurring Listeria species were found at the firm. There have been no confirmed reports of adverse reactions and the products were distributed to retail locations nationwide.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-061-2016-release

10. *July 20, Associated Press* – (Tennessee) **Destructive beetle found in White County; quarantine issued.** Tennessee officials issued a quarantine order for White County July 20 after an emerald ash borer was detected in the eastern section of the county. The quarantine prohibits the transportation of ash trees and ash tree products within the State.
Source: http://www.theeagle.com/news/nation/destructive-beetle-found-in-white-county-quarantine-issued/article_0625b542-10b1-5c47-9d2b-1aab0dda9af7.html

11. *July 19, U.S. Food and Drug Administration* – (National) **Faribault Foods, Inc., announces voluntary recall of a limited quantity of No-Salt-Added Black Beans due to the potential presence of foreign material.** Faribault Foods, Inc., issued a voluntary recall July 15 for a limited quantity of its No-Salt-Added Black Beans products sold in seven variations due to potential contamination with plastic and metal fragments after the company received a consumer complaint stating pieces of a pen were found in the products. No illnesses have been reported.
Source: http://www.fda.gov/Safety/Recalls/ucm511937.htm

For another story, see item **23**

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

See item **15**

Government Facilities Sector

12. *July 20, Softpedia* – (National) **DDoS attack takes down U.S. Congress Web site for three days.** A U.S. Library of Congress spokesperson reported that the U.S. Library of Congress, U.S. Copyright Office, and U.S. Congress Web sites were inaccessible July 17 – July 20 following a distributed denial-of-service (DDoS) attack involving a type of Domain Name System (DNS) attack that affected the infrastructure of the server hosting the Web sites. Officials reported the Web sites have recovered and no other U.S. Government portals appear to have been affected by the attack.
Source: http://news.softpedia.com/news/ddos-attack-takes-down-us-congress-website-for-three-days-506451.shtml

13. *July 19, KEVN 7 Rapid City* – (South Dakota) **Indian Canyon Fire now estimated at 14,133 acres.** Crews reached 60 percent containment July 19 of the 14,133-acre Indian Canyon Fire burning near Edgemont, South Dakota.
Source: http://www.blackhillsfox.com/content/news/Indian-Canyon-Fire-now-estimated-at-14133-acres-387484892.html

14. *July 19, Arizona Republic* – (Arizona) **Rain slows growth of Fuller Fire at Grand Canyon's North Rim.** Crews were working July 19 to contain the 14,131-acre Fuller Fire burning on the North Rim of the Grand Canyon in Arizona.
Source: http://www.azcentral.com/story/news/local/arizona/2016/07/19/rain-slows-growth-fuller-fire-grand-canyons-north-rim/87300906/

Emergency Services Sector

Nothing to report

Information Technology Sector

15. *July 20, SecurityWeek* – (International) **Oracle's critical patch update for July contains record number of fixes.** Oracle released its July Critical Patch Update (CPU) that addressed a total of 276 vulnerabilities in several of its products including 19 critical security flaws affecting the Oracle WebLogic Server component, the Hyperion Financial Reporting component, and the Oracle Health Sciences Clinical Development Center component, among other applications. The update also resolves 36 security flaws in applications specifically designed for the insurance, health, financial, and utility sectors, as well as 159 remote code execution (RCE) flaws that can be exploited without authentication.
Source: http://www.securityweek.com/oracle-addresses-276-security-flaws-19-critical-july-2016-cpu

16. *July 20, Softpedia* – (International) **Free decrypter available for Bart ransomware.** A security researcher for AVG released a free decrypter for the Bart ransomware that recovers files locked by the ransomware after discovering Bart uses one password for all files placed inside a password-protected ZIP archive.
Source: http://news.softpedia.com/news/free-decrypter-available-for-bart-ransomware-506469.shtml

17. *July 19, SecurityWeek* – (International) **Petya ransomware gets encryption upgrade.** A security researcher dubbed Hasherezade discovered the Petya ransomware no longer allows for easy data recovery after finding that the malware operators bundled Petya with Mischa, a failsafe designed to encrypt user files one at a time if Petya was unsuccessful in manipulating the Master Boot Record (MBR) to take over the boot process and encrypt the entire hard disk after a reboot.
Source: http://www.securityweek.com/petya-ransomware-gets-encryption-upgrade

18. *July 19, IDG News Service* – (International) **Security software that uses 'code hooking' opens the door to hackers.** Researchers from enSilo discovered 6 security

vulnerabilities affecting over 15 different products, including antivirus programs from Kapersky Lab, Trend Micro, and Symantec, among others, using hooking to intercept, monitor, or modify potentially malicious behavior in applications and operating systems (OS), can be exploited by malicious attackers to easily bypass the anti-exploit mitigations provided by Microsoft Windows or third-party applications in order to exploit the vulnerabilities and inject malicious code into any process running on a victim's device while remaining undetected .
Source: http://www.computerworld.com/article/3097202/security/security-software-that-uses-code-hooking-opens-the-door-to-hackers.html

19. *July 19, Softpedia* – (International) **Gmail security filters can be bypassed just by splitting a word in two.** Security researchers from SecureState discovered that an attacker can bypass Gmail's security features responsible for detecting malicious macros in Microsoft Office document attachments by separating "trigger words" into two words or across a row of text after finding that the security filters failed to detect malicious macros in the script when an attacker split a sensitive term on two different lines of the exploit code.
Source: http://news.softpedia.com/news/gmail-security-filters-can-be-bypassed-just-by-splitting-a-word-in-two-506447.shtml

20. *July 19, SecurityWeek* – (International) **DoS vulnerability patched in BIND.** The Internet Systems Consortium (ISC) released BIND versions 9.9.9-P2 and 9.10.4-P2 addressing a medium severity, remote code execution (RCE) vulnerability that could cause systems using the lightweight resolver protocol (lwresd) to resolve names to enter a denial-of-service (DoS) condition due to an error in the way the protocol was implemented after finding that the server can terminate when the lwresd is asked to resolve a query name that exceeds the maximum allowable length when combined with a search list entry.
Source: http://www.securityweek.com/dos-vulnerability-patched-bind

For another story, see item **12**

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

21. *July 20, SecurityWeek* – (National) **Data breach hits 140 Cicis restaurants.** Cicis restaurant reported July 19 that its point-of-sale (PoS) systems at 140 restaurant

locations were compromised after a March 2016 investigation revealed that attackers installed malware in its PoS systems in order to collect customers' payment information. Officials stated select restaurant locations were breached in 2015, while most attackers gained access to the PoS systems in 2016.
Source: http://www.securityweek.com/data-breach-hits-140-cicis-restaurants

22. *July 19, WPXI 11 Pittsburgh* – (Pennsylvania) **66 displaced after fire destroys entire building at Duquesne apartment complex.** The Laurel building at the Hilltop Parkview apartments in Duquesne, Pennsylvania, was considered a total loss July 19 following a fire that left 66 residents displaced and sent 2 firefighters to area hospitals for heat-related issues. The cause of the fire remains under investigation.
Source: http://www.wpxi.com/news/fire-at-duquesne-apartment-complex-destroys-entire-building/407303738

23. *July 19, WTVH 5 Syracuse* – (New York) **Employee accused of stealing $740k from White's Farm Supply since 2009.** A former employee at White's Farm Supply, Inc., in Lenox, New York, was charged July 19 after he allegedly embezzled over $740,000 from the company since 2009 by forging company checks and depositing them into his personal bank account.
Source: http://cnycentral.com/news/local/whites-farm-supply-employee-accused-of-stealing-740k-from-company-since-2009

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.