



Daily Open Source Infrastructure Report 18 August 2015

Top Stories

- The U.S. Federal Aviation Administration reported August 15 that a system problem at the Washington Air Route Control Center in Virginia forced the agency to temporarily halt area departures, leading to East Coast flight delays and cancellations. – *CNN* (See item [12](#))
- An August 15 fire destroyed a Washington College-leased building on Maryland’s Eastern Shore, causing \$3.5 million in estimated damages. – *Washington Post* (See item [17](#))
- The Industrial Control Systems Computer Emergency Response Team published six advisories covering multiple recently discovered vulnerabilities affecting Web-based Supervisory Control and Data Acquisition human machine interfaces. – *Securityweek* (See item [28](#))
- A sulfur dioxide leak at Hydrite Chemical Co., in Indiana August 15 prompted the evacuation of 200-300 spectators at the Hulman Mini Speedway and hospitalized at least 15 people. – *Associated Press* (See item [33](#))

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. *August 16, Los Angeles Times* – (California) **Homeless man arrested in 200-acre Montebello wildfire.** A 200-acre brush fire in Montebello, California forced the PXP oil field to cease all operations and closed all eastbound lanes of the 60 Freeway at San Gabriel Boulevard in Montebello for several hours August 16.
Source: <http://www.latimes.com/local/lanow/la-me-ln-brush-fire-montebello-20150816-story.html>
2. *August 15, WITI 6 Milwaukee* – (Wisconsin) **Power being restored to thousands after thunderstorm rips through SE Wisconsin.** More than 20,000 We Energies customers in Milwaukee, Wisconsin lost power August 14 after heavy winds and downed trees damaged power lines. As of August 15 fewer than 4,500 customers were still without power.
Source: <http://fox6now.com/2015/08/14/20000-without-power-after-severe-thunderstorm-rips-through-southeastern-wisconsin/>
3. *August 14, Detroit News* – (Michigan) **22,000 without power in Metro area after storms, winds.** Thunderstorms in southeast Michigan snapped tree limbs and downed electrical lines August 14, cutting power to 22,000 residents across St. Clair and Macomb counties in Michigan. Power was scheduled to be restored August 14.
Source: <http://www.detroitnews.com/story/news/local/macomb-county/2015/08/14/thousands-without-power-metro-area-storms/31760985/>
4. *August 14, KHOU 11 Houston; Associated Press* – (Texas) **Explosions, fire rock Texas chemical plant.** A series of explosions at the DrillChem plant in Conroe, an oil industry supply company, set off a 3-alarm fire which burned 2 hours August 14, prompting officials to issue a shelter-in-place order within a 2-mile radius of the site. No injuries were reported and the facility was empty at the time of the explosions.
Source: <http://www.cbsnews.com/news/explosions-fire-rock-texas-chemical-plant/>

For additional stories, see items [15](#) and [28](#)

Chemical Industry Sector

See items [4](#), [28](#), and [33](#)

Nuclear Reactors, Materials, and Waste Sector

See item [28](#)

Critical Manufacturing Sector

5. *August 15, Tech Times* – (National) **Mazda and Volkswagen recall more than 600,000 vehicles over loss of steering and airbag failure.** Volkswagen issued a recall for 420,000 model year 2010 – 2014 Tiguan, Passat, Jetta, GTI, Golf, CC, and Eos vehicles due to an issue in which debris could rip through a front air bag cable, leading

to a deployment failure. Mazda issued a separate recall for 193,000 model year 2007 – 2014 CX-9 vehicles due to an issue in which rust could cause front ball joints to fail, leading to a loss of steering

Source: <http://www.techtimes.com/articles/76883/20150815/mazda-and-volkswagen-recall-more-than-600-000-vehicles-over-loss-of-steering-and-airbag-failure.htm>

6. *August 14, San Jose Mercury News* – (California) **Fremont: Tesla plant temporarily closes after down power line.** Employees from Tesla Motors' Fremont plant were evacuated and the plant was shut down August 14 after a crane-truck damaged a power transmission line. PG&E officials reported that crews expected to have service restored August 14.

Source: http://www.mercurynews.com/business/ci_28641011/fremont-tesla-plant-closes-after-downed-power-line

7. *August 14, Threatpost* – (International) **OwnStar attack now aimed at BMW, Chrysler, Mercedes cars.** A security researcher who developed a Raspberry Pi-based device to intercept traffic between GM vehicles and the OnStar RemoteLink app reported that BMW, Mercedes-Benz, and Chrysler vehicles were also vulnerable to attacks due to similar respective mobile app failures to validate Secure Sockets Layer (SSL) certificates.

Source: <https://threatpost.com/ownstar-attack-now-aimed-at-bmw-chrysler-mercedes-cars/114283>

For another story, see item [28](#)

Defense Industrial Base Sector

See item [28](#)

Financial Services Sector

8. *August 17, U.S. Securities and Exchange Commission* – (National) **Citigroup affiliates to pay \$180 million to settle hedge fund fraud charges.** The U.S. Securities and Exchange Commission announced August 17 that Citigroup Global Markets Inc., and Citigroup Alternative Investments LLC (CAI) agreed to pay \$180 million to settle allegations that the affiliates failed to disclose risks associated with the ASTA/MAT and Falcon hedge funds, which raised almost \$3 billion from about 4,000 investors before collapsing, and that CAI accepted up to \$110 million in investments after the funds began to collapse.

Source: <http://www.sec.gov/news/pressrelease/2015-168.html>

For another story, see item [34](#)

Transportation Systems Sector

9. *August 17, WCPO 9 Cincinnati* – (Ohio) **Police identify driver killed in head-on crash on I-74.** Eastbound Interstate 74 in Cincinnati reopened August 17 after being

shut down for nearly 4 hours while officials investigated and cleaned up a head-on collision that killed 1 person.

Source: <http://www.wcpo.com/traffic/eastbound-interstate-74-closed-after-fatal-head-on-collision>

10. *August 16, WFSB 3 Hartford* – (Connecticut) **Investigation continues after a pair of serious crashes snarls traffic on I-95 for hours.** Interstate 95 northbound in Old Lyme, Connecticut, reopened August 15 after both directions of the highway were shut down for several hours following 2 separate crashes that injured 9 people and killed 2 others. The incidents are under investigation.
Source: <http://www.wfsb.com/story/29793602/i-95-southbound-closed-in-old-lyme>
11. *August 16, CNN* – (California) **2 small planes collide in midair in San Diego; 4 killed.** The U.S. Federal Aviation Administration (FAA) reported that 2 small planes crashed in midair in San Diego August 16, killing 4 people and starting a small brush fire that was later put out. Authorities are investigating the incident.
Source: <http://www.cnn.com/2015/08/16/us/small-planes-collide/index.html>
12. *August 15, CNN* – (National) **D.C., New York flight delays caused by air traffic glitch, FAA says.** The U.S. Federal Aviation Administration (FAA) reported August 15 that a problem with the system that processes flight plans at the Washington Air Route Control Center in Leesburg, Virginia, forced the agency to temporarily halt departures for all aircraft in the District of Columbia area's major airports, leading to flight delays and cancellations along the East Coast.
Source: <http://www.cnn.com/2015/08/15/travel/flight-delays-dc-new-york/>

For another story, see item [1](#)

Food and Agriculture Sector

13. *August 14, St. Louis Post-Dispatch* – (Missouri) **Rain Crow Ranch temporarily shuts down processing plant.** Missouri-based Rain Crow Ranch temporarily shut down production at its Jackson plant the week of August 3 until further notice following a Federal suspension that led to a shortage of the facility's grass-fed products for St. Louis grocers and restaurants. The plant will reopen once corrective actions are submitted and approved by the Food Safety and Inspection Service.
Source: http://www.stltoday.com/entertainment/dining/rain-crow-ranch-temporarily-shuts-down-processing-plant/article_49b50f63-74fc-506f-b7ea-e2d41ba40258.html
14. *August 14, U.S. Department of Agriculture* – (Illinois; Michigan) **Pleasant House Bakery recalls steak and chicken products distributed without the benefit of inspection and due to undeclared allergens.** The Food Safety and Inspection Service announced August 14 that Chicago-based Pleasant House Bakery, LLC issued a recall for an undetermined amount of steak and chicken pie products individually wrapped in 10-ounce packages due to undeclared eggs, milk, and wheat after the products were distributed without the benefit of inspection. The items were shipped to restaurants and retail stores in Chicago and New Buffalo, Michigan.

Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-111-2015-release>

Water and Wastewater Systems Sector

15. *August 17, KCAW 104.7 FM Sitka* – (Alaska) **Up to 7,000 gallons of diesel spilled from Sitka power plant.** A storage tank at Sitka’s Jarvis Street Diesel Plant failed over the weekend of August 15 and spilled an estimated 4,000 to 7,000 gallons of diesel fuel into the Sitka Sound near the mouth of the Indian River. Crews were investigating the cause of the failure and were working to contain and clean up the spill.
Source: <http://www.kcaw.org/2015/08/17/up-to-7000-gallons-of-diesel-spilled-from-sitka-power-plant/>

16. *August 16, Denver Post* – (New Mexico) **New Mexico, Utah drop water restrictions after Colorado mine spill.** New Mexico officials dropped San Juan County’s restrictions on using the Animas and San Juan rivers for drinking water August 15 after a 3 million gallon mine wastewater spill in Colorado caused by U.S. Environmental Protection Agency equipment August 5. Health officials are still warning the public to avoid sediment from the spill and to only catch and release fish until the impact to aquatic life is assessed.
Source: http://www.denverpost.com/news/ci_28649740/new-mexico-utah-drop-water-restrictions-after-colorado

For another story, see item [28](#)

Healthcare and Public Health Sector

See item [28](#)

Government Facilities Sector

17. *August 17, Washington Post* – (Maryland) **Damage estimated at \$3.5 million after fire at Maryland’s Washington College.** An August 15 fire destroyed a Washington College-leased administrative building on Maryland’s Eastern Shore, causing an estimated \$3.5 million in damage. The building was unoccupied during the incident and the cause of the fire remains under investigation.
Source: http://www.washingtonpost.com/local/crime/damage-estimated-at-35-million-after-fire-at-marylands-washington-college/2015/08/17/c35a8814-4497-11e5-8e7d-9c033e6745d8_story.html

18. *August 17, Idaho Statesman* – (Idaho) **Soda Fire 70 percent contained; fires in Idaho Panhandle tear through homes.** Crews reached 70 percent containment August 17 of the 283,686-acre Soda Fire burning in Owyhee County, Idaho. The cause of the fire remains under investigation.
Source: <http://www.idahostatesman.com/2015/08/17/3942172/soda-fire-70-percent-contained.html>

19. *August 17, San Francisco Bay City News* – (California) **Cabin Fire in Angeles National Forest 60 percent contained.** Crews reached 60 percent containment August 16 of the 1,470-acre Cabin Fire burning in the Angeles National Forest in California. Five structures were burned by the blaze and 10 firefighters suffered minor injuries. Source: <http://www.sgvtribune.com/general-news/20150816/cabin-fire-in-angeles-national-forest-60-percent-contained>
20. *August 17, KTVZ 21 Bend* – (Oregon) **Structure-protection crews leaving Warm Springs fire.** Crews reached 25 percent containment August 16 of the 59,150-acre Warm Springs Fire burning in Warm Springs, Oregon. Evacuation orders for several areas were downgraded while Kah-Nee-Ta Resort remained closed due to heavy smoke in the region. Source: <http://www.ktvz.com/news/47000acre-warm-springs-wildfire-at-still-raging/34741446>
21. *August 17, KCPQ 13 Tacoma* – (Washington) **More than 50 structures destroyed in Chelan fires; evacuations continue.** Firefighters worked August 16 to contain the Reach Complex fires which have burned over 55,000 acres in Chelan, Washington, and destroyed dozens of homes and one commercial building. Source: <http://q13fox.com/2015/08/16/chelan-fires-burn-55000-acres-some-power-restored/>
22. *August 16, KFSN 30 Fresno* – (California) **Rough Fire prompts evacuations for parts of Sierra National Forest.** Firefighters worked to contain the 16,000-acre Rough Fire burning in Fresno County, following mandatory evacuation orders for parts of the Sierra National Forest August 16. Source: <http://abc30.com/news/rough-fire-scorches-more-than-16000-acres-near-hume-lake/934385/>
23. *August 16, Charlottesville Daily Progress* – (Virginia) **UVa board hears about cyberattack, faculty hiring progress.** University of Virginia officials restored the school's computer network August 16 after shutting it down August 14 due to a cybersecurity threat that targeted the personal email accounts of 2 university employees. Faculty, students, and staff were urged to change their passwords after the network was brought back online. Source: http://www.dailyprogress.com/news/local/uva-board-hears-about-cyberattack-faculty-hiring-progress/article_6c8046fc-4472-11e5-9b22-3b3cfa4ab569.html
24. *August 14, WSMV 4 Nashville* – (Tennessee) **Police investigating threats made to multiple Midstate schools.** A series of threats at schools in Sumner, Maury, Robertson, Lewis, and Rutherford counties in Tennessee prompted evacuations and dismissals August 14 while police investigated. Nothing suspicious was found and authorities are probing the source of the threats. Source: <http://www.wsmv.com/story/29788311/police-investigating-threats-at-schools-in-murfreesboro-millersville>

25. *August 14, San Jose Mercury News* – (California) **Stanford: Knight Management Center reopens following bomb threat.** An August 14 bomb threat prompted the 6-hour closure of Stanford University's Graduate School of Business and Knight Management Center while police inspected the building and deemed it safe.
Source: http://www.mercurynews.com/spotlight/ci_28642313/stanfords-graduate-business-school-remains-closed-after-bomb?source=top_stories_bar
26. *August 14, WNBC 4 New York City* – (New Jersey) **11 kids taken to hospital after school bus crashes with SUV, smashes into liquor store.** Eleven Mt. Carmel Guild School children, the bus driver, and the driver of an SUV were injured after the school bus struck the SUV, and crashed into the side of a liquor store at a New Jersey intersection August 13. Authorities are inspecting the bus after the driver reported that the brakes failed prior to the crash.
Source: <http://www.nbcnewyork.com/news/local/Bus-Crash-Into-Building-Ivrington-New-Jersey-Injuries-Car-Crash-321740462.html>

Emergency Services Sector

27. *August 16, Associated Press* – (Pennsylvania) **3 inmates charged in Pennsylvania prison melee that injured 5 guards, prompted lockdown.** Authorities charged 3 inmates August 16 in connection to an April 28 disruption at State Correctional Institution-Houtzdale in Pennsylvania that left 5 guards injured and prompted a lockdown of the facility. Officials stated that additional arrests are pending.
Source: <http://www.therepublic.com/view/story/404f29dd02094175b469974daa6d141b/PA--Prison-Lockdown-Guards-Injured>

Information Technology Sector

28. *August 17, Securityweek* – (International) **Alerts issued for zero-day flaws in SCADA systems.** The Industrial Control Systems Computer Emergency Response Team (ICS-CERT) published six advisories after security researchers from Elastica discovered several remote and local file inclusion, weak password hashing, insecure authentication, hardcoded credentials, weak cryptography, and cross-site request forgery (CSRF) vulnerabilities, among others, affecting Web-based Supervisory Control and Data Acquisition (SCADA) human machine interfaces (HMI) used by multiple organizations.
Source: <http://www.securityweek.com/ics-cert-issues-alerts-zero-day-flaws-scada-systems>
29. *August 17, Securityweek* – (International) **BitTorrent flaws can be exploited for DRDoS attacks: researchers.** Security researchers reported that malicious actors could exploit vulnerabilities in BitTorrent's Micro Transport (uTP), Distributed Hash Table (DHT), and Message Stream Encrypton (MSE) protocols as well as its Sync tool to reflect and amplify traffic via distributed reflective denial-of-service (DRDoS).
Source: <http://www.securityweek.com/bittorrent-flaws-can-be-exploited-drdoS-attacks-researchers>

30. *August 17, Securityweek* – (International) **Exploit for OS X zero-day published by researcher.** A security researcher published a proof of concept (PoC) for a local privilege escalation vulnerability in Apple’s OS X Yosemite dubbed “tpwn”, which could be executed by leveraging two security bugs to gain root privileges using a specially crafted file
Source: <http://www.securityweek.com/exploit-os-x-zero-day-published-researcher>
31. *August 15, Softpedia* – (International) **Administrators continue to fail in securing databases by using proper configs.** Security researchers from BinaryEdge released analysis of 4 technologies including Redis, MongoDB, Memcached, and ElasticSearch, revealing that almost 1.2 petabytes (PB), or 1,175 terabytes (TB) of data were vulnerable due to administrators’ use of default configurations that do not block connections from untrusted external actors.
Source: <http://news.softpedia.com/news/administrators-continue-to-fail-in-securing-databases-by-using-proper-configs-489322.shtml>

For another story, see item [23](#)

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

See item [28](#)

Commercial Facilities Sector

32. *August 16, KARE 11 Minneapolis* – (Minnesota) **Dozens displaced after Lakeville motel fire.** An August 16 fire at the Friendly Host Inn in Lakeville, Minnesota, left more than 40 residents displaced after crews found the blaze in a third floor apartment unit and extinguished it. Nine firefighters were treated for heat exhaustion, and an investigation is ongoing to determine the cause of the fire.
Source: <http://www.kare11.com/story/news/2015/08/16/dozens-displaced-after-lakeville-motel-fire/31820067/>
33. *August 16, Associated Press* – (Indiana) **15 treated at hospital after Terre Haute chemical leak.** A sulfur dioxide leak at Hydrite Chemical Co., in Terre Haute, Indiana, August 15 prompted the evacuation of 200-300 spectators at the nearby Hulman Mini Speedway racetrack and sent at least 15 people to area hospitals for respiratory issues including nasal irritation, nausea, and difficulty breathing. The leak was contained after several hours.
Source: <http://www.indystar.com/story/news/2015/08/16/treated-hospital-terre-haute->

[chemical-leak/31825833/](#)

34. *August 15, WMAR 2 Baltimore* – (Maryland) **Bomb threat force Annapolis evacuations.** Three businesses including two Sun Trust Banks and one Giant Food Store in Annapolis were evacuated for more than 2 hours August 15 after the businesses received consecutive bomb threats, demanding monetary funds. Police searched the three facilities and cleared the scene once nothing suspicious was found. Source: <http://www.abc2news.com/news/crime-checker/anne-arundel-crime/bomb-threats-force-annapolis-evacuations>

35. *August 14, Cleveland.com* – (Ohio) **100 evacuated from Westlake hotel after bomb threat.** The Courtyard by Marriott hotel in Westlake, Ohio, was evacuated for 2 hours August 14 after the hotel received 2 computer-generated phone calls claiming that there was a bomb and 4 armed individuals inside the building. Authorities responded and cleared the scene once nothing suspicious was found. Source: http://www.cleveland.com/westlake/index.ssf/2015/08/100_evacuated_from_westlake_ho.html

For additional stories, see items [20](#) and [21](#)

Dams Sector

See item [28](#)



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.