



Daily Open Source Infrastructure Report 07 July 2015

Top Stories

- All lanes of Interstate 85 in Anderson County reopened July 3 after being shut down for nearly 9 hours while HAZMAT crews responded to the incident. – *Anderson Independent-Mail* (See item [11](#))
- Orlando Health announced July 2 that about 3,200 patients’ records were compromised at Winnie Palmer Hospital for Women and Babies, Dr. P. Phillips Hospital, and Orlando Regional Medical Center . – *Orlando Sentinel* (See item [15](#))
- Officials reported July 5 that the Arizona State Prison Complex-Kingman brought in 96 members of its special tactical unit to restore order following several riots. – *USA Today* (See item [18](#))
- FireKeepers Casino Hotel in Battle Creek, Michigan reported July 3 that its main computer system was compromised and may have affected 85,000 customers’ credit and debit cards. – *Battle Creek Enquirer* (See item [34](#))

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 5, WWLP 22 Springfield* – (Massachusetts) **Section of road closed due to gas leak and repairs.** A natural gas leak was discovered in a manhole on Hickory Street in Springfield, Massachusetts July 4, prompting officials to close the corner of Hickory and Allen streets until repairs could begin. Columbia Gas crews began replacing the gas main July 5, and expect the replacement to be completed by July 7.
Source: <http://wwlp.com/2015/07/05/road-closed-due-to-gas-leak/>

[\[Return to top\]](#)

Chemical Industry Sector

2. *July 5, NBC News* – (Texas) **Huge fire at Texas chemical facility prompts warning to residents.** Texas authorities reported July 5 that a 12-alarm fire at the Flowchem plant in Waller County prompted a 2-mile shelter-in-place order July 4. No injuries were reported and HAZMAT crews responded and cleaned the area.
Source: <http://www.nbcnews.com/news/us-news/residents-told-shelter-place-after-fire-texas-chemical-facility-n386881>

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[\[Return to top\]](#)

Critical Manufacturing Sector

3. *July 2, CNBC* – (National) **Ford recalls 433K vehicles amid body control module issues.** Ford Motor Company announced a recall July 2 for 433,000 model year 2015 Focus, C-MAX, and Escape vehicles due to an issue with body control module software in which engines could stay on after the ignition key is turned to the “off” position.
Source: <http://www.cnbc.com/id/102752192>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

4. *July 3, KTTV 11 Los Angeles; Cybercast News Service* – (California) **Fullerton ‘Bandit’ linked to six bank robberies in Orange County.** FBI officials are searching for a suspect dubbed the “Big A Bandit” who allegedly robbed a Bank of the West in Fullerton, California July 2 and is believed to be linked to 5 other Orange County bank robberies since 2013.
Source: <http://www.myfoxla.com/story/29467560/fullerton-suspect-linked-to-six-bank-robberies-in-orange-county>
5. *July 2, St. Paul Pioneer Press* – (Illinois) **Developers accused in \$16M mortgage fraud.** Two Glenview real estate developers and 4 alleged co-conspirators were indicted July 1 on charges alleging that they caused over \$16 million in losses to banks, mortgage lenders, Fannie Mae, and Freddie Mac by falsely promoting condominiums at “The Woods at Countryside” in Palatine by promising impossible financial incentives, and that they conspired to conceal and misrepresent facts from banks and mortgage lenders to approve nonconforming loans.
Source: <http://www.chicagotribune.com/suburbs/mundelein/news/ct-mun-mortgage-fraud-tl-0709-20150702-story.html>
6. *July 2, Associated Press* – (New York) **NYPD: 17 charged in counterfeit credit card scheme.** New York Police Department officials reported July 2 that 17 suspects were charged in connection with an alleged credit card counterfeiting ring that used stolen debit and credit card information to encode blank cards, which would be used to purchase items in New York City stores.
Source: <http://www.washingtontimes.com/news/2015/jul/2/nypd-17-charged-in-counterfeit-credit-card-scheme/>

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

[\[Return to top\]](#)

Transportation Systems Sector

7. *July 5, NBC News* – (Kentucky) **Ohio River capsizes: two dead, search for three missing continues.** The Coast Guard reopened almost 4 miles of the Ohio River near Louisville, Kentucky, July 5 while crews searched for 3 missing people after a boat carrying 9 people capsized, killing 2 of them July 4. Authorities are investigating the incident.
Source: <http://www.nbcnews.com/news/us-news/ohio-river-capsize-louisville-officials-say-two-dead-three-missing-n386896>
8. *July 5, Denver Post* – (Colorado) **Oil tanker crash spilled oil near Colorado River, closes I-70.** Interstate 70 in western Colorado along the Colorado River was shut down for several hours July 5 while crews cleared the roadway after an oil tanker overturned and spilled 30 gallons of oil. Authorities are investigating the cause of the accident.
Source: http://www.denverpost.com/environment/ci_28437725/oil-tanker-crash-spilled-oil-near-colorado-river

9. *July 5, KYW 1060 AM Philadelphia* – (Pennsylvania) **All lanes of I-95 reopen after accident shuts down section in Delaware County.** All lanes of Interstate 95 in Delaware County have reopened July 5 after being closed for approximately 5 hours while crews responded to a multi-vehicle accident that involved a semi-truck, 2 other vehicles, and injured 3 people.
Source : <http://philadelphia.cbslocal.com/2015/07/05/accident-shuts-down-stretch-of-i-95-in-delaware-county/>
10. *July 4, TravelPulse.com*– (International) **Delta cargo hold fire scare causes emergency landing.** Delta Flight DL-71 headed to Atlanta from Amsterdam with almost 400 passengers onboard was diverted to Shannon Airport in Co. Clare, Ireland July 4 after an alarm regarding a potential fire went off. Thousands of gallons of fuel were dumped and the cargo area’s fire extinguishers were activated but officials determined there was no evidence of fire onboard.
Source: <http://www.travelpulse.com/news/impacting-travel/delta-cargo-hold-fire-scare-causes-emergency-landing.html>
11. *July 3, Anderson Independent-Mail* – (South Carolina) **Tanker wreck shuts down miles of Interstate 85 for hours.** All lanes of Interstate 85 in Anderson County reopened July 3 after being shut down for nearly 9 hours while HAZMAT crews responded to an accident that involved a vehicle and a semi-truck carrying a flammable material called polyurethane, spilled onto the highway. No injuries were reported.
Source: <http://www.independentmail.com/news/wreck-involving-2-18-wheelers-has-i-85n-blocked>

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

[\[Return to top\]](#)

Food and Agriculture Sector

12. *July 6, U.S. Food and Drug Administration* – (National) **Whole Foods Market’s Southwest region recalls Cherry, Blackberry and Peach pies in four stores due to undeclared egg.** An Austin, Texas-based Whole Foods Market is recalling its Cherry, Blackberry, and Peach pies due to an undeclared egg allergen July 2. The products were produced and sold in four retail stores in Texas, Oklahoma, and California.
Source: <http://www.fda.gov/Safety/Recalls/ucm453662.htm>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

13. *July 5, Fort Myers News-Press* – (Florida) **Boil water notice affects 2,000 in Lehigh Acres.** A 12-inch water main was damaged July 5 following a car accident that cut water services to more than 2,000 Lehigh Acres residents and prompted a preliminary boil water notice that may remain until July 8. Crews are working to restore service.
Source: <http://www.news-press.com/story/news/2015/07/05/boil-water-notice-affects->

[\[Return to top\]](#)

Healthcare and Public Health Sector

14. *July 5, CNN* – (Colorado) **1 dead, 2 injured after medical helicopter crashes at hospital in Colorado, catches fire.** A Flight for Life helicopter crashed in the parking lot of the St. Anthony Summit Medical Center in Frisco, Colorado July 3, killing the pilot and injuring two others on board. Authorities are investigating the cause of the crash.
Source: <http://fox13now.com/2015/07/05/1-dead-2-injured-after-medical-helicopter-crashes-at-hospital-in-colorado-catches-fire/>
15. *July 2, Orlando Sentinel* – (Florida) **Orlando Health reports data breach for 3,200 patients.** Orlando Health announced July 2 that about 3,200 patients' records were compromised after a former employee improperly accessed insurance information for patients at Winnie Palmer Hospital for Women and Babies, Dr. P. Phillips Hospital, and Orlando Regional Medical Center between January 2014 --- May 2015. Officials say there is no evidence that the information has been misused.
Source: <http://www.orlandosentinel.com/business/brinkmann-on-business/os-orlando-health-data-breach-20150702-post.html>
16. *July 2, Monthly Prescribing Reference* – (National) **Recall: Antipsychotic found in bottle labeled for GERD medication.** AstraZeneca announced a voluntary recall of 34,524 mislabeled Nexium bottles following the discovery of Seroquel XR, an antipsychotic agent, in an unopened Nexium container.
Source: <http://www.empr.com/safety-alerts-and-recalls/nexium-recall-seroquel-xr/article/424512/>

[\[Return to top\]](#)

Government Facilities Sector

For another story, see item [21](#)

[\[Return to top\]](#)

Emergency Services Sector

17. *July 6, WDRB 41 Louisville* – (Kentucky) **Police seize guns, drugs, cash, body armor in west Louisville after suspect allegedly threatened officers.** A Louisville man was arrested and charged July 5 for allegedly threatening to murder several police officers, trafficking in marijuana, and possessing drug paraphernalia, among other charges, after he approached a police vehicle fully armed and threatened police.
Source: [http://www.wdrb.com/story/29481817/police-seize-guns-drugs-cash-body-](http://www.wdrb.com/story/29481817/police-seize-guns-drugs-cash-body-armor-in-west-louisville-after-suspect-allegedly-threatened-officers)

[armor-in-west-louisville-after-suspect-allegedly-threatened-officers](#)

18. *July 5, USA Today* – (Arizona) **Ariz. sends special forces to quell Kingman prison riot.** Officials reported July 5 that the Arizona Department of Corrections brought in 96 members of its special tactical unit to restore order after a series of disturbances and riots began from July 2 -- July 4 that injured 9 staff members and 7 inmates at the Arizona State Prison Complex-Kingman. The incident has been resolved and officials stated that 700 inmates will be transferred to other prisons.
Source: <http://www.usatoday.com/story/news/nation/2015/07/05/quell-kingman-prison-riot/29741193/>
19. *July 3, Associated Press* – (Ohio) **Police bosses charged in pursuit that ended in 137 shots fired.** Five Cleveland police supervisors were charged for misdemeanors July 2 for allegedly failing to stop a 22-mile car chase that ended in a massive police shooting and the deaths of two suspects in November 2012.
Source: <http://www.policeone.com/suspect-pursuit/articles/8645497-Police-bosses-charged-in-pursuit-that-ended-in-137-shots-fired/>

[\[Return to top\]](#)

Information Technology Sector

20. *July 6, Securityweek* – (International) **KINS malware toolkit leaked online.** Security researchers from MalwareMustDie reported that version 2.0 of the KINS banking trojan toolkit was leaked and widely distributed on the Internet, and that the malware's developers have integrated ZeusVM banking trojan technology in the newest release, including the use of stenography to conceal configuration data.
Source: <http://www.securityweek.com/source-code-kins-malware-toolkit-leaked-online>
21. *July 6, Softpedia* – (International) **Govt supplier of surveillance software gets hacked, 400GB of data leaked.** The Italian surveillance software company, Hacking Team reported that its systems were hacked, and 400 gigabytes of corporate data was leaked to the public. The company developed products for government agencies worldwide, including the U.S. Drug Enforcement Agency and the FBI.
Source: <http://news.softpedia.com/news/supplier-of-govt-surveillance-software-gets-hacked-400gb-of-data-leaked-486099.shtml>
22. *July 4, Softpedia* – (International) **Matsnu backdoor uses RSA crypto on exfiltrated data.** Security researchers from Check Point discovered malware dubbed Matsnu, also known as Androm backdoor and Boxed.DQH, which acts as a backdoor on compromised machines, and sends Rivest-Shamir-Adleman (RSA)-encrypted user and system information back to a command and control (C&C) server.
Source: <http://news.softpedia.com/news/matsnu-backdoor-uses-rsa-crypto-on-exfiltrated-data-486039.shtml>
23. *July 4, Softpedia* – (International) **TYPO3 Enterprise CMS update adds 7 security fixes.** TYPO3 released an update for its Enterprise Content Management System

(CMS) addressing 7 security fixes for cross-site scripting (XSS) and authentication vulnerabilities, as well as the addition of login protection against brute-force attacks. Source: <http://news.softpedia.com/news/typo3-enterprise-cms-update-adds-7-security-fixes-486027.shtml>

24. *July 4, Softpedia* – (International) **Node.js fixes denial of service bug.** Developers released an update for Node.js addressing a bug affecting all Buffer to Strings conversions in which a triggered out-of-band write in Google Chrome’s JavaScript runtime V8 engine UTF-8 decoder could lead to a denial of service (DoS) condition. Source: <http://news.softpedia.com/news/node-js-fixes-denial-of-service-bug-486019.shtml>
25. *July 3, Softpedia* – (International) **Dungarees Web site hacked, card information exposed.** Dungaree reported that the company’s Web site had been hacked, and that customers who placed orders from March 26 – June 5 may have had their card-related data compromised, including card verification values (CVV). Dungaree secured the Web site and is offering identity theft protection services to affected customers. Source: <http://news.softpedia.com/news/dungarees-website-hacked-card-information-exposed-485993.shtml>
26. *July 3, Securityweek* – (International) **Mozilla patches critical vulnerabilities with release of Firefox 39.** Mozilla released version 39 of Firefox addressing 24 issues, including 3 use-after-free vulnerabilities, 7 critical uninitialized memory, buffer overflow, unowned memory, poor validation issues, 3 critical memory safety browser engine bugs, and high-severity privilege escalation, and type confusion flaws. Source: <http://www.securityweek.com/mozilla-patches-critical-vulnerabilities-release-firefox-39>
27. *July 3, Securityweek* – (International) **Ad fraud trojan Kovter patches Flash player, IE to keep other malware out.** A security researcher from Kafeine reported that the Kovter ad fraud trojan has been updating Adobe Flash Player and Microsoft Internet Explorer on infected systems in an effort to exclude other malware platforms. Source: <http://www.securityweek.com/ad-fraud-trojan-kovter-patches-flash-player-ie-keep-other-malware-out>

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>

[\[Return to top\]](#)

Communications Sector

28. *July 5, KXAS 5 Dallas-Fort Worth* – (Texas) **Nearly 800 without phone service,**

internet service in Seagoville. Nearly 800 Seagoville residents were without phone or Internet access after an accident on U.S. Highway 175 damaged an AT&T terminal box. AT&T is working to restore services and the cause of the accident remains unknown.

Source: <http://www.nbcdfw.com/news/local/Nearly-800-Without-Phone-Service---Outage-in-Seagoville-311675271.html>

[\[Return to top\]](#)

Commercial Facilities Sector

29. *July 6, BBC News* – (Florida) **Florida: tourists from Ireland caught up in ‘lightning strike’ fire at resort.** The Avanti International Resort in Orlando, Florida evacuated approximately 500 units after lightning struck the building’s roof and started a blaze July 5. Fire crews contained the incident and no injuries were reported
Source: <http://www.bbc.com/news/uk-northern-ireland-33412038>
30. *July 6, WFLA 8 Tampa* – (Florida) **Fire destroys businesses at Largo shopping center.** A June 5 fire in Largo, Florida destroyed several businesses in a shopping center including Kern’s Fireplace Restaurant, Debbie Allen’s Salon, and three surrounding businesses. Florida officials believe fireworks may be the cause of the incident.
Source: <http://wfla.com/2015/07/06/fire-destroys-businesses-at-largo-shopping-center/>
31. *July 6, WMBF 32 Myrtle Beach* – (South Carolina) **Fire engulfs Pentecostal church in Scotland County.** A July 5 fire at the Woodville Pentecostal Holiness Church in Scotland County prompted multiple fire agencies from surrounding counties to respond to the incident. Total damages are unknown and no injuries were reported.
Source: <http://www.foxcarolina.com/story/29479538/full-engulfed-pentecostal-church-fire-in-scotland-county>
32. *July 5, KGO 7 San Francisco* – (California) **4-alarm fire burns 320 acres near Pena Adobe Park in Vacaville.** A 4-alarm bush fire in Vacaville, California closed Lagoon Valley and Pena Adobe parks and prompted the evacuation of approximately 100 homes July 4. Fire crews extinguished the blaze and the cause of the incident is under investigation.
Source: <http://abc7news.com/news/4-alarm-fire-burns-320-acres-near-keating-park-in-vacaville/829246/>
33. *July 4, KFMB 8 San Diego; Cybercast News Service* – (California) **Fire forces evacuations at La Mesa apartment complex.** A 2-alarm fire displaced more than half a dozen residents from a La Mesa apartment complex after the flames began in the kitchen of a unit and spread to surrounding areas. An investigation is ongoing to determine the cause of the incident and damages total \$325,000.
Source: <http://www.cbs8.com/story/29474753/fire-forces-evacuations-at-la-mesa-apartment-complex>

34. *July 3, Battle Creek Enquirer* – (Michigan) **FireKeepers data breach affects about 85,000.** FireKeepers Casino Hotel in Battle Creek, Michigan reported July 3 that its main computer system was compromised from September 2014 – April 2015, and may affect approximately 85,000 credit and debit cards, as well as private information on customers and employees. The casino replaced its point-of-sale (PoS) equipment and is offering credit monitoring and identity protection services to those affected.
Source: <http://www.wzzm13.com/story/news/local/2015/07/03/firekeepers-casino-confirms-data-breach/29669543/>

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



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.