



Daily Open Source Infrastructure Report 26 November 2012

Top Stories

- A crucial 200-mile stretch of the Mississippi River may be on the verge of shutdown to barge traffic, a move that could paralyze commerce on a vital inland waterway and ultimately drive up consumer prices. – *USA Today* (See item [6](#))
- Testing by the U.S. Food and Drug Administration on steroid medications produced by the New England Compounding Center found more contaminants in additional drugs. – *Nashville Tennessean* (See item [21](#))
- Nearly 50 female inmates at a York County, Pennsylvania prison were treated for carbon monoxide poisoning. Officials said a preliminary investigation indicated the deadly odorless and colorless gas may have come from the heating, ventilation, and air conditioning system. – *Associated Press* (See item [23](#))
- Internet service was restored November 21 for Charter Communication customers after vandals cut a fiber-optic cable, crashing service across northern California for about 18 hours. The outage affected local Internet service providers and the City of Redding’s systems as well. – *Redding Record Searchlight* (See item [33](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

Energy Sector

1. *November 21, Reuters* – (Louisiana; International) **US regulator warns Black Elk on safety after rig fire.** The U.S. Bureau of Safety and Environmental Enforcement (BSEE) November 21 ordered Black Elk Energy to take immediate steps to improve safety at its offshore platforms, after a deadly rig explosion off the Louisiana coast killed one worker and left another missing the week of November 12. “Black Elk has repeatedly failed to operate in a manner that is consistent with federal regulations,” the director of the BSEE said in a statement. In a letter, the offshore regulator said Houston-based Black Elk’s performance “must be improved immediately,” and gave it until December 15 to submit a plan. The November 16 explosion and fire occurred when workers were welding a pipe on the deck of West Delta Block 32 platform, which sits in 56 feet of water about 17 miles south of Grand Isle, Louisiana. The Black Elk chief executive said in a statement that the company has received the letter and “We will be in full cooperation with all agencies.”

Source: <http://www.reuters.com/article/2012/11/21/usa-offshore-fire-idUSL1E8ML40D20121121>

For another story, see item [6](#)

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

Chemical Industry Sector

Nothing to report

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

Nuclear Reactors, Materials and Waste Sector

Nothing to report

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

Critical Manufacturing Sector

2. *November 21, Reuters* – (International) **Toyota recalls 160,000 Tacoma pickups in U.S. and Canada.** Toyota Motor Corp announced November 21 the recall of about 160,000 Tacoma mid-size pickup trucks from model years 2001 to 2004 in 20 cold-weather U.S. States and in Canada because the spare tire could fall off. The spare tire in these Tacoma models is stored beneath the trucks’ bed. When the trucks were made, the metal plate that keeps the spare tire in place was not coated with sufficient amounts of phosphate to retard rust, Toyota said. Two accidents have been reported to Toyota involving vehicles following a Tacoma truck. Over time and in limited cases, corrosion of the plate could cause it to break, causing the detachment of the spare tire. Letters

will go to the owners of the recalled vehicles in December, and Toyota dealers will replace the spare tire assembly, if necessary.

Source: <http://wkzo.com/news/articles/2012/nov/21/toyota-recalls-160000-tacoma-pickups-in-us-and-canada/>

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

Defense Industrial Base Sector

Nothing to report

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

Banking and Finance Sector

3. *November 23, Silicon Republic* – (International) **Fake Apple invoices in your inbox could lead to empty bank accounts.** Fake Apple invoices are appearing in inboxes that contain a Blackhole exploit kit and a trojan that is designed to log users' keystrokes and ultimately compromise bank accounts, Silicon Republic reported November 23. The multi-pronged approach was discovered by a Sophos researcher who reported it in the Naked Security blog. The online criminals who circulated the fake invoices are using a form of social engineering where users think they are being billed for an expensive product they never bought, in the researcher's case, he received an invoice telling him he ordered and paid for goods valued at \$699. If a user clicks on any of the links contained in the email they are taken to a page proclaiming to be the IRS telling them their browser is unsupported and offers a range of browser options. As the page is displayed, the user's computer gets infected with the Zeus/Zbot trojan. If the user clicks on any of the browser options, a file labeled update.exe is downloaded. If the user opens the file their computer is automatically infected with the trojan, which is designed to record keystrokes and ultimately give criminals the information they need to access the user's bank account online.

Source: <http://www.siliconrepublic.com/strategy/item/30388-fake-apple-invoices-in-your/>

4. *November 23, The H* – (International) **DDoS attackers cost PayPal 3.5 million pounds.** PayPal paid around \$5.6 million to defend and arm itself against distributed denial-of-service (DDoS) attacks, The H reported November 23. The attacks in 2010 and 2011 were named Operation Payback by members of hacktivist collective Anonymous. The details were revealed in a court case in the United Kingdom where a defendant is facing charges of conspiring to impair the operation of computers. The BBC reported the prosecution as saying that more than one hundred workers from eBay, PayPal's parent company, spent 3 weeks working on DDoS-attack-related issues and that PayPal had bought software and hardware to defend itself against further attacks.

Source: <http://www.h-online.com/security/news/item/DDoS-attackers-cost-PayPal-Lb3-5-million-1755947.html>

Transportation Sector

5. *November 23, Associated Press* – (Pennsylvania) **5 hurt in head-on crash with SEPTA bus in Philly.** Five people were injured in a head-on crash involving a bus and a car in Philadelphia November 23. They said the driver of a sedan appeared to be under the influence when he lost control and collided with a SEPTA bus. WPVI reported the driver of the car was rushed to a hospital in critical condition and was upgraded to stable condition. Four people on the bus were treated for minor injuries. Source: <http://www.timesunion.com/news/article/5-hurt-in-head-on-crash-with-SEPTA-bus-in-Philly-4061649.php>

6. *November 23, USA Today* – (National) **Mississippi River commerce imperiled by low water.** A crucial 200-mile stretch of the Mississippi River may be on the verge of shutdown to barge traffic, a move that could paralyze commerce on a vital inland waterway and ultimately drive up consumer prices. The temporary closure of the Mississippi River from St. Louis to Cairo, Illinois, could result from an Army Corps of Engineers plan to reduce water flow from a reservoir into the Missouri River starting November 23, shipping companies and industry groups warned. The Corps annually decreases water releases to ensure adequate reservoir levels and to prevent ice buildup and flooding. In 2012, already-low river levels caused by drought could shrink to the point that barges carrying grain, coal, and other products would not be able to navigate the Mississippi, said a spokesperson with the Waterways Council, which represents ports and shippers. “This is an impending economic crisis that could delay shipment of \$7 billion in commodities in December and January,” she said. A Corps spokeswoman said water releases from the reservoir at Gavins Point Dam on the Nebraska-South Dakota border will drop gradually starting November 23 from 36,000 cubic feet per second to 12,000 by December 11. Due to the drought, most vessels on the Mississippi River are now limited to a 9-foot draft, said a spokesperson with Knight Hawk Coal. “If we go to 6-foot drafts, the river is effectively closed,” he said. Source: <http://www.firstcoastnews.com/news/usworld/article/283549/6/Mississippi-River-commerce-imperiled-by-low-water>

7. *November 22, Associated Press* – (Texas) **Texas highway pileup: Massive car crash shuts I-10 in Texas; at least 2 dead.** Two people died and more than 80 people were hurt November 22 when at least 140 vehicles collided in southeast Texas in a pileup that left trucks twisted on top of each other and authorities rushing to pull survivors from the wreckage. The collision occurred in extremely foggy conditions November 22 on Interstate 10 southwest of Beaumont, Texas. A man and a woman were killed in a vehicle crushed by a tractor trailer, the Texas Department of Public Safety (DPS) said. A Jefferson County sheriff’s deputy said in a news release that 80 to 90 people were transported to hospitals with 10 to 12 of those in serious to critical condition. He said 140 to 150 vehicles were involved in the pileup. According to DPS, a crash on the eastbound side of the highway led to other accidents in a dangerous chain reaction. There were multiple crashes on the other side of the highway as well. I-10’s eastbound lanes were re-opened November 22 after more than 8 hours.

Source: http://www.huffingtonpost.com/2012/11/22/texas-highway-pileup-crash_n_2175909.html

8. *November 21, New York Times* – (New York; New Jersey) **Train service at Penn Station partially restored after switching problem.** A switch malfunction brought train traffic out of New York City’s Pennsylvania Station to a standstill for over an hour November 21, causing delays and rankling thousands of holiday travelers on one of the busiest travel days of the year. All service — including Amtrak, New Jersey Transit, and Long Island Rail Road trains — was shut down for about 1 and 1/2 hours, railroad officials said. Thousands of people squeezed into waiting areas, to the point where at times it was difficult to move. A spokesman for the Long Island Rail Road, said the issue was “an electrical problem that has affected a switch or switches right at the point where trains leave or enter Penn.” Amtrak and New Jersey Transit customers faced delays of 60 to 90 minutes, railroad officials said.

Source: <http://cityroom.blogs.nytimes.com/2012/11/21/all-train-service-at-penn-station-shut-down-due-to-switching-problem/>

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

Postal and Shipping Sector

Nothing to report

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

Agriculture and Food Sector

9. *November 21, Associated Press* – (California) **State plans Tulare Co. quarantine for citrus pest.** California officials plan to quarantine an area in the State’s citrus belt where a pest capable of killing citrus trees was found. A California Department of Food and Agriculture spokesman said November 20 that the State is working to determine the quarantine’s boundaries in Tulare County. The quarantine will go into effect the week of November 26. An Asian citrus psyllid was discovered the week of November 12 in a commercial citrus orchard in the county. The psyllid can spread a bacteria capable of killing citrus trees. Officials were not able to determine whether the psyllid found near Strathmore was carrying the bacteria. The spokesman said that in other psyllid quarantines, only commercially cleaned and packed citrus fruit may be moved out of a quarantine area.

Source: <http://www.thebusinessjournal.com/news/agriculture/4046-state-plans-tulare-co-quarantine-for-citrus-pest>

10. *November 21, Food Safety News* – (National) **Cherry tomatoes recalled for possible Salmonella.** Rio Queen Citrus announced November 21 the recall of 840 cartons of Dry Pints of Mexican cherry tomatoes in “Karol” brand boxes due to possible Salmonella contamination. According to Rio Queen, the tomatoes were distributed through retail stores in Texas and South Carolina. However, according to WOWT 6 Omaha, the tomatoes were also distributed to Nebraska, Iowa, Missouri, Illinois,

Kansas, South Dakota, Minnesota, and Wisconsin. The product was originally distributed in a bulk container of 12/1 Dry Pints in boxes labeled “Karol” with the Lot No. “01W45” stamped in the upper, right-hand corner on the face of the box. The box states “Distributed by Interstate Fruit & Vegetable”, which is an affiliated business of Rio Queen Citrus, Inc. The tomatoes were distributed to stores between November 10 and November 19 and may have been repackaged by individual retailers. The contamination was discovered through routine testing by the U.S. Food and Drug Administration.

Source: [http://www.foodsafetynews.com/2012/11/cherry-tomatoes-recalled-for-possible-salmonella/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+food+safetynews/mRcs+\(Food+Safety+News\)](http://www.foodsafetynews.com/2012/11/cherry-tomatoes-recalled-for-possible-salmonella/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+food+safetynews/mRcs+(Food+Safety+News))

11. *November 20, U.S. Food and Drug Administration* – (National) **Carolina Prime Pet Inc. announces recall of Priority Total Pet Care All Natural Bullstrips because of possible Salmonella health risk.** Carolina Prime Pet Inc., a manufacturer and distributor of dog treats, announced a voluntarily recall November 20 of Priority Total Pet Care All Natural Bullstrips in a 5-count package. The product yielded a positive test for Salmonella when tested by the Colorado Department of Agriculture. Salmonella can affect animals eating the products and there is risk to humans from handling contaminated pet products, especially if they have not thoroughly washed their hands after having contact with the products or any surfaces exposed to these products. Priority Total Pet Care All Natural Bullstrips are sold in Safeway stores in Arizona, California, Colorado, Delaware, Hawaii, Maryland, Nebraska, Nevada, New Mexico, South Dakota, Virginia, Washington D.C., and Wyoming, as well as Vons, Pavilions, and Pak ‘N Save stores in California; Randalls and Tom Thumb stores in Texas; Genuardi’s stores in Pennsylvania and New Jersey; and Dominick’s stores in Illinois. The product was distributed from about the first of September until November 20. Source: <http://www.fda.gov/Safety/Recalls/ucm329165.htm>
12. *November 20, U.S. Food and Drug Administration* – (National) **Voluntary precautionary product recall: Sara Lee Butter Streusel Coffee Cake for undeclared allergens.** Sara Lee voluntarily initiated a product recall November 20 of Sara Lee Butter Streusel Coffee Cake with a best by date of October 16, 2013, as a precautionary measure because the product may contain pecans, an undeclared allergen, that are not listed on the label. This national recall affects 3,381 pounds of product with the best by date on the side panel. Source: <http://www.fda.gov/Safety/Recalls/ucm329216.htm>

For another story, see item [6](#)

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

Water Sector

13. *November 23, Associated Press* – (West Virginia) **Drought affects 3 WV lakes’ fall drawdown.** Extreme drought conditions across the Greater Mississippi Valley are

affecting the fall drawdown of three lakes in West Virginia, the Associated Press reported November 23. The U.S. Army Corps of Engineers said it was temporarily halting the fall drawdown of Sutton and Summersville lakes. The start of Bluestone Lake's drawdown was already delayed. The Corps said the drawdown adjustments are necessary due to expected low water levels on the lower Ohio River and points downstream. Drawdown of the three lakes will resume December 1. They are expected to reach winter pool by December 10.

Source: <http://www.statejournal.com/story/20169047/drought-affects-3-wv-lakes-fall-drawdown>

14. *November 21, Austin American-Statesman* – (Texas) **Partially-treated sewage spilled into Plum Creek near Kyle.** The company that operates Kyle, Texas's wastewater treatment plant announced November 20 that more than 100,000 gallons of partially-treated sewage spilled into Plum Creek. Officials with Aqua Texas, which is responsible for maintaining and operating the city's treatment plant, said the spill happened sometime between November 15 and November 19. The spill was discovered November 20, said the vice president of operations at Aqua Texas. He estimated that vacuum trucks had sucked about three-quarters of the spill by November 21. Solids are no longer spilling from the plant, and the company expected to be done cleaning the creek November 21 before moving back inside the facility to finish cleaning up there, he said. He said the spill does not affect the drinking water supply, and that no dead fish have been found in the stream.

Source: <http://www.statesman.com/news/news/local/partially-treated-sewage-spilled-into-plum-creek-n/nTCmm/>

15. *November 21, Baltimore Sun* – (Maryland) **Baltimore County sewage spill from Sandy belatedly detected.** A broken sewer line in Catonsville, Maryland, went undetected for 3 weeks after Hurricane Sandy passed through the area, poured nearly 1.3 million gallons of raw waste into a tributary of the Patapsco River, Baltimore County officials reported November 21. County workers discovered the spill November 20 on the grounds of Spring Grove Hospital Center after a neighboring resident complained about sewage odors to the Maryland Department of the Environment, which relayed the information, according to a spokesman for the county's Department of Public Works. A tree that officials believe was uprooted by Sandy broke the 8-inch sewer line, and it apparently escaped notice after the October 30 storm because the rupture occurred in a wooded portion of the State psychiatric facility's 200-acre campus. A utility crew installed a temporary bypass around the broken pipe November 20. Until then, officials estimated that the break had been spilling about 60,000 gallons of sewage a day into the West Branch of Herbert Run, which flows into the Patapsco. Until test results are obtained, a spokeswoman recommended that residents avoid contact with Herbert Run and with the Patapsco downriver from where the creek joins it.

Source: <http://www.baltimoresun.com/features/green/blog/bs-gr-sewage-spill-herbert-run-20121121,0,5540652.story>

For another story, see item [6](#)

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

Public Health and Healthcare Sector

16. *November 23, Associated Press* – (Indiana) **Indiana chickenpox outbreak largest in US, official says.** The chief medical officer of the Indiana Department of Health said western Indiana's Vigo County is experiencing the largest known current outbreak of chickenpox in the U.S., the Associated Press reported November 23. The chief medical officer told the Terre Haute Tribune-Star that Vigo County usually has less than 10 cases per year. The county reported 84 cases since September. She said it is not clear why the county is having such a large outbreak. Vigo County School Corp. officials excluded 230 students from school the week of November 12 because of the outbreak. Source: <http://www.foxnews.com/us/2012/11/23/indiana-chickenpox-outbreak-largest-in-us-official-says/>
17. *November 22, United Press International* – (Pennsylvania) **Legionnaires' disease in Pittsburgh VA hospital has fifth victim.** A fifth person was by sickened by the Legionnaires' disease outbreak linked to a Pittsburgh-area hospital's water supply, a hospital spokesman said. The outbreak was traced to the water distribution system at the Veterans Administration Pittsburgh Healthcare System University Drive Campus, the Pittsburgh Tribune-Review said November 22. Hospital officials said the week of November 12, four patients who developed pneumonia caused by the Legionella bacteria were successfully treated and released. A VA spokesman said the patient likely contracted the illness before officials finished cleaning the hospital's water system by hyperchlorination and flushing. The hospital has imposed water restrictions since the outbreak began November 16, and officials have brought in bottled water for drinking and bagged water for bathing. Officials determined the fifth patient was infected at the hospital, basing the conclusion on the incubation period for the bacteria. Source: http://www.upi.com/Top_News/US/2012/11/22/Fifth-Legionnaires-victim-in-Pittsburgh/UPI-35661353613644/
18. *November 22, Sturgis Journal* – (Michigan) **Mich.: 13 dead, 167 cases in meningitis outbreak.** Officials said the Michigan death toll from a national meningitis outbreak rose to 13, with at least 167 infections reported. The Michigan Department of Community Health said November 21 that the State has had 67 cases of meningitis, including the 13 deaths. In addition, there have been 91 epidural abscesses, one stroke, and eight joint infections. The fungal meningitis is linked to contaminated steroids produced by a Massachusetts pharmacy used in injections for neck or back pain. Four deaths were from Livingston County and two from Washtenaw County, with one each in Cass, Charlevoix, Genesee, Ingham, and Wayne counties. Two other deaths involved Michigan residents infected in Indiana. Source: <http://www.sturgisjournal.com/article/20121122/NEWS/121129888>
19. *November 22, KVIA 7 El Paso* – (Texas) **Sierra Medical Center reopens after electrical fire.** Sierra Medical Center (SMC) in El Paso, Texas, reopened November 22 after it was closed following a fire in its electrical room. Initially, three floors were evacuated November 21, but after a few hours the entire building was closed because of

electrical issues. Investigators said the electrical fire caused a power outage. A spokesperson for SMC said dozens of patients had to be evacuated to nearby hospitals and each patient was transferred with an SMC staff member who was in possession of the patients' chart.

Source: <http://www.kvia.com/news/Sierra-Medical-Center-reopens-after-electrical-fire/-/391068/17525618/-/104b14f/-/index.html>

20. *November 21, Boston Globe* – (Massachusetts) **State regulators: Hospitals may share drugs to avoid shortages following meningitis outbreak.** Massachusetts public health regulators November 21 adopted emergency regulations that will allow hospitals to share medications to address drug shortages created by the closure of two specialty pharmacies following a national outbreak of fungal meningitis. The rules adopted by the State's public health council, an appointed board of professors, clinicians, and public health advocates, will go into effect December 1. The policy and health planning director at the Department of Public Health told the council November 21 that hospitals were reporting shortages of certain medications before the outbreak. But, he said, the shortages have increased since their closures in October. The rules are primarily aimed at allowing hospitals to share drugs within their health care systems. But the State could consider special requests to distribute them outside those organizations.

Source: <http://www.boston.com/whitecoatnotes/2012/11/21/state-regulators-hospitals-may-share-drugs-avoid-shortages-due-meningitis-outbreak/QepRMCLs4IEyimlYMSIYI/story.html>

21. *November 21, Nashville Tennessean* – (National) **Meningitis outbreak: FDA finds more contaminants in NECC meds.** Testing by the U.S. Food and Drug Administration (FDA) on steroid medications produced by New England Compounding Center has found more contaminants in additional drugs, the Nashville Tennessean reported November 21. The FDA has updated its list of lot numbers for contaminated drugs after finding unknown fungal growths in triamcinolone and bethamethasone. It also found three forms of bacteria in betamethasone and one form of bacteria in trimacinolone. New England Compounding Center's products have been linked to a national outbreak of fungal meningitis and other infections that have sickened 490 people, with 34 deaths. Tennessee has had the most deaths with 13 and the second-most illnesses with 82. This is the first time that the FDA has confirmed contaminants in triamcinolone. However, the agency previously said in an inspection report that foreign substances were found on heating and cooling vent louvers behind a piece of equipment used to make bulk drug suspensions of preservative-free methylprednisolone and triamcinolone.

Source:

http://www.tennessean.com/article/20121121/NEWS07/311210144/Meningitis-outbreak-FDA-finds-more-contaminants-NECC-meds?odyssey=mod|newswell|text|FRONTPAGE|p&gcheck=1&nclick_check=1

For another story, see item [15](#)

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

Government Facilities Sector

22. *November 21, Federal Times* – (National) **White House issues insider threat guidance to agencies.** The White House November 21 issued new minimum standards for agencies to guard against insider security threats such as those that led to a 2010 breach. In a memo, the U.S. President directed agencies to install programs to thwart internal threats, including espionage, violent acts against the government, and unauthorized disclosures of classified information and sensitive data stored on government computer networks and systems. According to the memo, minimum standards for a government-wide insider threat program should include: The ability to gather, integrate, and centrally analyze and respond to key threat-related information, the ability to monitor employees' use of classified networks, insider threat awareness workforce training, and protections of civil liberties and privacy of all personnel.

Source:

<http://www.federaltimes.com/article/20121121/AGENCY04/311210002/White-House-issues-insider-threat-guidance-agencies>

For more stories, see items [16](#), [17](#), and [33](#)

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

Emergency Services Sector

23. *November 22, Associated Press* – (Pennsylvania) **49 female inmates sickened by gas at Pa. prison.** Nearly 50 female inmates at a York County, Pennsylvania prison were treated for carbon monoxide poisoning. A statement from York County said five inmates remained hospitalized as of November 22. The remaining 44 were returned to the York County Prison. The women fell ill November 21 in a prison dormitory. Officials said a preliminary investigation indicated the deadly odorless and colorless gas may have come from the heating, ventilation, and air conditioning system. That system was shut down. The county's statement said carbon monoxide levels have returned to normal. Prisoners living in the affected unit were relocated to other areas in the facility.

Source:

http://www.google.com/hostednews/ap/article/ALeqM5iWnMC3qY_jBrba0wSdXICqqaEmbA?docId=aff8ec4e6a09455fa42c48a4806acbf3

24. *November 22, Associated Press* – (Iowa) **Man accused of faking emergency calls.** A man was accused of faking emergency calls and jamming or otherwise disrupting the Des Moines, Iowa police department's radio frequency, the Associated Press reported November 22. He was charged with 28 counts of obstructing emergency communications and 8 counts of impersonating public officials. KCCI 8 Des Moines reported that police said he made calls in November that forced the dispatch of officers, vehicles, and equipment to the scenes of nonexistent incidents. Police said he would also leave his radio set on the police frequency without talking on it, tying up the channel. It is legal to monitor emergency communications, but accessing the system

and making false transmissions is illegal. He was arrested November 20 at his home after police tracked his location from transmissions.

Source: <http://www.kcrg.com/news/local/Man-Accused-of-Faking-Emergency-Calls-180521211.html>

25. *November 21, Modesto Bee* – (California) **Calif. farm inmates set fires to get home for Christmas.** Inmates at the Stanislaus County Honor Farm in California intentionally set two recent fires in an attempt to get home for Christmas, the sheriff said. The fires — one November 17 and the second November 19, both in the inmate barracks — caused only minor damage and disruption to the facility, the sheriff said November 20, crediting staff and firefighters with quick response. The sheriff said the inmates believed that if they burned down the barracks, there would not be anywhere to house them and officials would have no choice but to let them go. The inmates have been shifted to other locations and procedures were tweaked to prevent further fires. Source: <http://www.firehouse.com/news/10832644/calif-farm-inmates-set-fires-to-get-home-for-christmas>

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

Information Technology Sector

26. *November 23, Krebs on Security* – (International) **Yahoo email-stealing exploit fetches \$700.** A zero-day vulnerability in yahoo.com that lets attackers hijack Yahoo! email accounts and redirect users to malicious Web sites offers a fascinating glimpse into the underground market for large-scale exploits. The exploit, being sold for \$700 by an Egyptian hacker on an exclusive cybercrime forum, targets a “cross-site scripting” (XSS) weakness in yahoo.com that lets attackers steal cookies from Yahoo! Webmail users. Such a flaw would let attackers send or read email from the victim’s account. “I’m selling Yahoo stored xss that steal Yahoo emails cookies and works on ALL browsers,” wrote the vendor of this exploit, using the hacker handle ‘TheHell.’ “And you don’t need to bypass IE or Chrome xss filter as it do that itself because it’s stored xss.” Krebs On Security alerted Yahoo! to the vulnerability, and the company says it is responding to the issue. The director of security at Yahoo! said the challenge now is working out the exact yahoo.com URL that triggers the exploit. Source: <http://krebsonsecurity.com/2012/11/yahoo-email-stealing-exploit-fetches-700/>
27. *November 23, Softpedia* – (International) **Cybercriminals use fake digital certificates to sign police trojans.** Cybercriminals have begun using fake certificates to sign ransomware to ensure that the malware have a better chance of evading digital signature checks. Trend Micro experts have come across a couple of samples, identified as TROJ_RANSOM.DDR, both signed with a suspicious name and issued by a suspicious provider. One of the samples relies on the FBI to scare internauts into paying a fine if they want to see their computers unlocked, while the other one uses the reputation of the UK’s Police Central e-Crime Unit. The newer variants lock up computers and threaten victims with messages based on their geographic location. The language used to demand the payment of fines is adapted and so is the name of the law enforcement agency.

Source: <http://news.softpedia.com/news/Cybercriminals-Use-Fake-Digital-Certificates-to-Sign-Police-Trojans-309128.shtml>

28. *November 23, Softpedia* – (International) **Sucuri warns of fake jQuery sites distributing malware.** Cybercriminals have set up a number of fake jQuery Web sites and are using them to distribute pieces of malware. Experts from Sucuri Malware Labs have identified at least three such sites. The jquerys.org, jquery-framework.com, and jqueryc.com domains are the ones in question. According to researchers, references to jqueryc.com have been found in the header of the index.php file of numerous sites. Users are advised to steer clear of such sites. The legitimate jQuery sites are jquery.com and jquery.org. Other variants, even if they look legitimate, are likely fake. Source: <http://news.softpedia.com/news/Sucuri-Warns-of-Fake-jQuery-Sites-Distributing-Malware-309189.shtml>
29. *November 23, Softpedia* – (International) **Cybercriminals hack DNS records of Go Daddy sites to distribute ransomware.** Cybercriminals have found a clever way to distribute pieces of ransomware by hacking the Domain Name System (DNS) records of Web sites hosted by Go Daddy in an effort to redirect visitors to their own malicious sites. According to researchers from security firm Sophos, crooks are abusing this system by adding their own IP addresses to the DNS records of Web sites. By adding several subdomains with corresponding DNS entries that reference malicious IPs, attackers can evade security filtering and trick users into thinking that they are on a legitimate site. In this particular case, the rogue servers to which users are redirected to host an exploit kit called Cool EK, which looks for vulnerabilities in the target system to distribute ransomware. Experts have not been able to determine if the attackers are utilizing stolen account credentials, because Go Daddy does not allow webmasters to view their historical login activity. Source: <http://news.softpedia.com/news/Cybercriminals-Hack-DNS-Records-of-Go-Daddy-Sites-to-Distribute-Ransomware-309327.shtml>
30. *November 23, Softpedia* – (International) **ENISA releases report on the use of honeypots to detect cyberattacks.** Digital traps or honeypots are often used by security researchers to detect and analyze cyber threats. However, according to the European Network and Information Security Agency (ENISA), their usage among Computer Emergency Response Teams (CERTs) is not as widespread as it should be. In a previous report, entitled “Proactive Detection of Network Security Incidents,” ENISA detailed the benefits of using honeypots to detect and investigate attacks. Despite their efficiency, certain CERTs have not deployed them. That is why the new study focuses on a number of 30 honeypots to offer insight on which technologies and solutions should be utilized. The report also looks at critical issues organizations are confronted with and practical deployment strategies. Over the past years, honeypots have been successfully utilized on a number of occasions. These digital traps are designed to mimic a real service, an application, or a system in an attempt to lure potential cyberattackers. When an entity connects to a honeypot, it is automatically considered to be suspicious and its every move is closely monitored in an attempt to detect malicious activity.

Source: <http://news.softpedia.com/news/ENISA-Releases-Report-on-the-Use-of-Honeypots-to-Detect-Cyberattacks-309270.shtml>

31. *November 22, Softpedia* – (International) **Experts find way to crack default WPA2 passwords of Belkin routers.** Security researchers claim that the default WPA2 passwords used by many Belkin routers can be easily guessed by an attacker who knows the device's WAN MAC address. A number of Belkin wireless routers are shipped with a default WPA2 password to protect network connections. The apparently random passwords are printed on a label on the bottom of the router. Although this approach should in theory be more secure, because the password is likely stronger than what many users would set themselves, it turns out that the random passphrases are not so random. The researchers determined that the password is based on the device's WAN MAC address, and since this information is not so difficult to obtain, a remote attacker could easily hack into a targeted network if the default configuration is used. The default password is made of 8 characters which can be determined by replacing each hex-digit of the WAN MAC address with another value from a static substitution table. Several device models are affected, including Belkin N450 Model F9K1105V2 and Belkin Surf N150 Model F7D1301v1.

Source: <http://news.softpedia.com/news/Experts-Find-Way-to-Crack-Default-WPA2-Passwords-of-Belkin-Routers-309081.shtml>

32. *November 21, Softpedia* – (International) **Exploitation of privileged access points: Common vector for high-profile attacks.** A study performed by information security firm Cyber-Ark labs reveals that, in most of the recent high-profile cyberattacks, the common attack vector is the exploitation of privileged access points. These privileged access points usually consist of administrative or privileged accounts, application backdoors, and hardcoded or default passwords. In recent months, privileged access points have been utilized in the Flame attacks, and the ones against companies such as Saudi Aramco and Subway. The executive vice president Americas of Cyber-Ark Software explains that cybercriminals are well aware of the power and wide ranging access provided by these access points, which is the main reason why future attacks will also target them.

Source: <http://news.softpedia.com/news/Exploitation-of-Privileged-Access-Points-Common-Attack-Vector-for-High-Profile-Attacks-308594.shtml>

For another story, see item [4](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@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: <https://www.it-isac.org>

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

Communications Sector

33. *November 21, Redding Record Searchlight* – (California) **Vandals cut Charter Communications’ cable; crash Internet for 18 hours.** Internet service was restored November 21 for Charter Communication customers after vandals cut a fiber-optic cable, crashing service across northern California for about 18 hours. The cable was cut near Emeryville near Oakland. The outage halted email service and online bill payment services for all City of Redding departments. Charter officials said they did not know how many customers were affected. A spokeswoman for Charter said Comcast customers and local Internet service providers were also impacted by the disruption of service. The cable was cut by vandals November 20, which sent workers scurrying to repair the damage, a CenturyLink spokeswoman said November 21. Crews spliced the fiber line to make the repairs. Work was slowed because of flooding in the area, which sent water into manholes where the cable was located.
Source: <http://www.redding.com/news/2012/nov/21/vandals-cut-charter-communications-cable-crash/>

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

Commercial Facilities Sector

34. *November 23, Associated Press* – (Missouri) **5 people die in apartment fire in SW Missouri.** Five people died after a fire broke out at an apartment building in southwest Wheaton, Missouri, authorities said. The chief of the Wheaton Fire Department told the Associated Press the fire was reported November 22. Fire crews arrived at the apartment within minutes of getting the call and found the victims in two separate units at the building. The fire was fully involved when firefighters arrived from the fire station located a few blocks away. Two adults and a child were found in one apartment and the two other adults were found in a nearby apartment in the building, which is one of two eight-unit buildings in the apartment complex, he said. The second building was not affected, but residents were evacuated as a precaution. The Red Cross of Southern Missouri said it was providing 16 people with emergency lodging, food and clothing. It has opened five cases for financial assistance.
Source: http://abclocal.go.com/wtvd/story?section=news/national_world&id=8895949
35. *November 22, Los Angeles Daily News* – (California) **Man’s body found after fire at Canoga Park strip mall.** A victim’s body was found in a burned-out business that went up in flames in Canoga Park, California, November 22. A Los Angeles Fire Department spokesman did not know how the fire started. “Right now the fire remains under investigation by the Los Angeles City Fire Department’s arson investigators,” he said. “But, so far, there is no indication that this was an arson fire.” One of 62 firefighters assigned to the fire fell off a ladder was taken to a hospital to be checked out, he said. Three units at the strip mall were severely damaged, and three sustained damage in areas where they shared walls, a videographer at the scene said.
Source: http://www.dailynews.com/ci_22047352/mans-body-found-after-fire-at-canoga-park?source=most_viewed
36. *November 22, Associated Press* – (Washington) **A few dozen displaced after Skyway apartment fire.** More than 30 people were displaced after a fire burned through an

apartment building in Skyway, Washington. A Skyway Fire spokesman said firefighters responded to a call November 22 at the Greentree Apartment Homes. They encountered heavy smoke coming from a third-story unit. He said one unit was completely destroyed and another had heavy fire and smoke damage. Two units had water damage and three units had smoke damage. He said due to the age of the building, sprinklers were not required. The Seattle Red Cross and the City of Renton opened the Renton Community Center as a shelter location for those displaced by the fire.

Source: <http://www.ktvz.com/news/A-few-dozen-displaced-after-Skyway-apartment-fire/-/413192/17524554/-/nf56bgz/-/index.html>

37. *November 21, WTVQ 36 Lexington* – (Kentucky) **Update: Meth arrest inside Walmart.** Walmart employees in Nicholasville, Kentucky, called police November 21 and asked them to check on an incoherent man who had been in the bathroom a long time. When police arrived they say they found a suspect passed out, while also holding meth and producing it. “When they searched his backpack that he had with him they saw what appeared to be a mobile Meth lab actively cooking in his backpack, which obviously was a potentially volatile situation,” said a Nicholasville Police spokesperson. Police evacuated the store, and shut it down for 2 hours while detectives cleaned up the meth lab. The police charged the suspect with manufacturing meth, possessing meth, and possessing drug paraphernalia.

Source: <http://www.wtvq.com/content/localnews/story/Meth-Arrest/AsvodrK7MkuL2xb-7EUsLg.csp>

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

National Monuments and Icons Sector

38. *November 21, Los Angeles Times* – (California; National) **Yosemite hantavirus outbreak has sickened 10, killed 3, CDC says.** To date, 10 people have fallen ill — and 3 have died — in the hantavirus outbreak at California’s Yosemite National Park’s “signature” cabins in Curry Village, according to the U.S. Centers for Disease Control and Prevention (CDC), the Los Angeles Times reported November 21. At Yosemite, deer mice infected with the Sin Nombre strain of hantavirus took up residence in the insulation in the signature cabins. Nine of the 10 human hantavirus cases occurred in guests who had stayed in the cabins, researchers from State public health agencies, the National Park Service and the CDC said in a brief article issued November 21 in the CDC’s Morbidity and Mortality Weekly Report. The researchers also reported that the 10 patients came from California, Pennsylvania, and West Virginia, and were between 12 and 56 years of age. Nine had typical symptoms of hantavirus pulmonary syndrome, such as fever, chills, and aching. There is no treatment for hantavirus pulmonary syndrome, but receiving intubation, supplemental oxygen, and other supportive care can boost survival rates. The Yosemite cabins have been closed since August 28. The National Park Service is making changes to park facilities to help prevent future hantavirus outbreaks.

Source: <http://www.latimes.com/health/boostershots/la-heb-hantavirus-yosemite-cdc-update-20121121,0,6821344.story>

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

Dams Sector

39. *November 23, Sacramento Bee* – (California) **Fire burns in plant linked to Oroville Dam.** A large fire burned November 22 in one of the hydroelectric generating units connected to Oroville Dam on the Feather River in California, the Sacramento Bee reported November 23. The fire began in the Thermalito Pumping-Generating Plant, downstream of Oroville Dam at Thermalito Forebay. The facilities are operated by the California Department of Water Resources (DWR) and are part of the State Water Project, which delivers water as far south as San Diego. No one was injured in the fire, which was believed to have started in the control room, said a California Department of Forestry and Fire Protection captain. Automatic extinguishers in the room were activated but were unable to contain the blaze. There were 38 firefighters and 10 engines working the blaze in the five-story power plant structure, including personnel from Cal Fire and the Oroville and Chico fire departments. Damage would likely be extensive to the equipment in the building and the structure itself, said a DWR spokesman. At one point, firefighters had to retreat because equipment began to collapse and heavy smoke caused zero visibility. No power outages were expected or any water shortages for customers of the State Water Project.

Source: <http://www.modbee.com/2012/11/23/2466757/fire-burns-in-plant-linked-to.html>

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



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)387-2341
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.