



## Daily Open Source Infrastructure Report 29 November 2012

### Top Stories

- IT experts reported security flaws in pacemakers and defibrillators could be putting lives at risk, stating that many devices are not properly secured and therefore are vulnerable to hackers who may want to commit an act that could lead to multiple deaths, Homeland Security reported November 28. – *Homeland Security News Wire* (See item [21](#))
- The International Atomic Energy Agency said information stolen from one of its former servers was posted on a hacker Web site November 27, and it was taking “all possible steps” to ensure its computer systems and data were protected. – *Reuters* (See item [6](#))
- Authorities said 30 Tennessee counties received false bomb threats to courthouses or other government buildings November 27, forcing evacuations while authorities conducted searches. – *Associated Press* (See item [23](#))
- A Texas hotel claimed to have suffered multiple burglaries stemming from flaws in a common type of electronic lock, exploits for which were demonstrated at this year’s Black Hat hacking conference, the Register reported November 27. – *The Register* (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

See item [19](#)

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

## Chemical Industry Sector

1. *November 28, KTVZ 21 Bend* – (Oregon) **Cement smothers Prineville zirconium fire.** A spark from a shovel ignited a fire in a pit of flammable zirconium in an industrial area west of Prineville, Oregon, November 27, officials said. The blaze sent up a tall smoke plume for hours, prompting authorities to keep students and anyone with respiratory problems indoors. The chief of Crook County Fire and Rescue said the fire was reported at EnviroTech Services. The company makes de-icer, and “zirconium is a byproduct of their process,” the fire chief said. “Zirconium, when it’s dried in a form of metal filings, is highly flammable. If a spark or something is near it, it can catch fire.” The material is located in a “not incredibly deep” containment pit, the fire chief said, adding that “everything worked as it should have,” in terms of isolating the fire in the pit and preventing more problems. Fire officials said the company learned from a similar fire in 2011. After that incident, a pit was dug to hold the metal shavings of zirconium. “The containment pit worked as it was supposed to, and the fire was contained to that.” A hazardous materials team from SMAF Environmental was called in and began pouring dry cement onto the fire to smother it. The fire marshal said a spark from a shovel or scoop on a machine ignited the pile of metal filings. The fire department worked in close coordination with the Crook County Emergency Management Director, as well as the sheriff’s office, health department, Pioneer Memorial Hospital, and area schools.  
Source: <http://www.ktvz.com/news/Cement-smothers-Prineville-zirconium-fire/-/413192/17566544/-/30gfcz/-/index.html>
2. *November 27, Rock Hill Herald* – (South Carolina) **Heater ignites fire at Fort Mill chemical plant.** Fire burned at the Nation Ford Chemical Plant in Fort Mill, South Carolina, November 27 after oil in a heating unit ignited, producing thick, black smoke and forcing several employees to evacuate. Company employees were performing maintenance on a heating unit when oil used for heating processes caught fire. The unit was not running at the time. The fire caused about \$100,000 in damage. Nation Ford Chemical produces “colorants for plastics, polymers,” the company president said. The plant was expected to reopen that night. A contract welder from Rock Hill Industrial Piping and Fabrication said the fire started in the rear of the plant and that firefighters from Fort Mill, Flint Hill, Riverview, Pleasant Valley, and Indian Land fire departments quickly had it under control. Though the oil was nontoxic, the Fort Mill fire chief said it had the potential to cause damage if the unit was operating and the oil reached its “high heat.” He ruled the fire as an accidental mechanical failure.  
Source: <http://www.heraldonline.com/2012/11/27/4442575/crews-called-to-fire-at-fort-mill.html>

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

## Nuclear Reactors, Materials and Waste Sector

3. *November 28, Reuters* – (International) **South Korea finds more nuclear parts with fake documents.** South Korean nuclear regulators have discovered nearly a thousand more parts supplied for nuclear power plants with fake quality certificates, they said November 28, adding that this would not lead to further reactor shutdowns. Revelations that fake certificates were supplied by eight firms forced the shutdown of two of the country's 23 reactors in November, raising the risk of winter power shortages. A third reactor was subjected to an extended maintenance period after microscopic cracks were found in tunnels that guide control rods. Nuclear normally accounts for a third of South Korea's power supplies. The Nuclear Safety and Security Commission said further investigation had uncovered 919 parts of 53 items supplied by two new firms with forged quality documents. Most had been fitted in six reactors — five of which were already affected by the earlier revelations. The country's sole power transmitter and distributor, Korea Electric Power Corp, said it would hold a drill November 28 to check for stable power supply and gauge the chances of outages this winter.  
Source: <http://www.nucpros.com/content/south-korea-finds-more-nuclear-parts-fake-documents>
4. *November 27, Reuters* – (New Jersey) **Exelon completes nozzle work at NJ Oyster Creek reactor.** U.S. power company Exelon Corp completed repairs on a reactor vessel nozzle at the Oyster Creek nuclear power plant in New Jersey, federal nuclear regulators said November 27. "The company's weld overlay repairs to a reactor vessel nozzle found recently to have two 'indications' (flaws or defects) are now completed," a spokesman for the U.S. Nuclear Regulatory Commission (NRC) said in an email. November 26, Exelon said the 615-megawatt plant was in a safe shutdown mode and it would fix the nozzle before the reactor could exit a refuelling outage. The company however, did not say when the 43-year old unit would exit the outage, which began October 22. Exelon told the NRC in an event report November 27 it found a pinhole leak of about 2 to 3 drops per minute during testing of the reactor head spray line. The leak was through an earlier weld. The NRC said the line was part of a reactor vessel head cooling system, which is only used when the plant is shutting down. The company said it was investigating the cause of the leak and developing a plan to fix the problem.  
Source: <http://www.reuters.com/article/2012/11/27/utilities-operations-exelon-oyster-idUSL1E8MR68I20121127>
5. *November 27, Bloomberg* – (Maryland) **Constellation shuts Calvert Cliffs nuclear plant for work.** Constellation Energy Group Inc. shut the 873-megawatt Calvert Cliffs 1 reactor near Annapolis, Maryland, for unplanned work on control element assemblies. Extensive monitoring at the unit, which slowed to 45 percent of capacity November 27 and halted, showed "traces of electrical noise" with one of the coils in the No. 37 assembly, said a plant spokesman. Crews were replacing the coils and conducting more tests on all assembly equipment, he said. Constellation has been monitoring electrical coils at Unit 1 since the summer of 2012, when the equipment failed and caused a reduction in output. The coils hold up control rods and allow operators to insert those rods into the core to slow or boost output. Calvert Cliffs Unit 2 continues to operate at full power.

Source: <http://www.bloomberg.com/news/2012-11-27/constellation-shuts-calvert-cliffs-nuclear-plant-for-work.html>

6. *November 27, Reuters* – (International) **U.N. atom agency says stolen information on hacker site.** The U.N. nuclear watchdog said information stolen from one of its former servers had been posted on a hacker Web site November 27, and it was taking “all possible steps” to ensure its computer systems and data were protected. The stolen information was contained in a statement by a hacking group. The International Atomic Energy Agency (IAEA) said the theft concerned “some contact details related to experts working” with the Vienna-based agency but it did not say who might have been behind the action. A Western diplomat said the stolen data was not believed to include information related to confidential work carried out by the IAEA. The statement posted under the name “Parastoo” included a large number of email addresses. An IAEA spokeswoman said the agency “deeply regrets this publication of information stolen from an old server that was shut down some time ago”. “The IAEA’s technical and security teams are continuing to analyze the situation and do everything possible to help ensure that no further information is vulnerable,” she said.

Source: <http://www.reuters.com/article/2012/11/27/net-us-nuclear-iaea-hacking-idUSBRE8AQ0ZY20121127>

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

## **Critical Manufacturing Sector**

Nothing to report

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

## **Defense Industrial Base Sector**

Nothing to report

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

## **Banking and Finance Sector**

7. *November 28, WBBM 2 Chicago* – (Illinois) **‘Stringer Bell Bandit’ robs Citibank branch in Loop.** Authorities are now linking a bank robbery in Chicago’s Loop area November 26 to the Stringer Bell Bandit — a man who allegedly robbed six other banks in seven attempts since October. The bandit — named after a character from the TV series *The Wire* — allegedly robbed the Citibank branch at 111 West Jackson Boulevard, according to the FBI’s Bandit Tracker Web site. He allegedly passed a note to the teller demanding cash, then fled on foot. No weapon was displayed. The Stringer Bell bandit allegedly struck the same bank November 13, according to the FBI.

Source: <http://chicago.cbslocal.com/2012/11/28/stringer-bell-bandit-robs-citibank-branch-in-loop/>

8. *November 27, IDG News Service* – (International) **Romanian authorities dismantle cybercrime ring responsible for \$25M credit card fraud.** Romanian law enforcement authorities dismantled a criminal group that stole credit card data from foreign companies as part of an operation that resulted in fraudulent transactions totaling \$25 million, IDG News Service reported November 27. Officers from the country's organized crime police working with prosecutors from the Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT) executed 36 search warrants and arrested 16 individuals suspected of being members of the credit card fraud ring. According to DIICOT, the group's members gained unauthorized access to computer systems belonging to foreign companies that operate gas stations and grocery stores, and installed computer applications designed to intercept credit card transaction data. The applications were configured to store the captured data locally for later retrieval, upload it automatically to external servers, or send it to email addresses controlled by the gang's members, the agency said. The stolen credit card information was then sold or used to create counterfeit cards. The group opened several IT services companies in Romania and used them for the specific purpose of building and maintaining a computer infrastructure that would support its criminal operation. A spokeswoman confirmed that the companies targeted by the fraud ring were not from Romania, but declined to name them or reveal in which countries they operate because the investigation is ongoing.

Source:

[http://www.computerworld.com/s/article/9234057/Romanian\\_authorities\\_dismantle\\_cybercrime\\_ring\\_responsible\\_for\\_25M\\_credit\\_card\\_fraud](http://www.computerworld.com/s/article/9234057/Romanian_authorities_dismantle_cybercrime_ring_responsible_for_25M_credit_card_fraud)

9. *November 27, U.S. Commodity Futures Trading Commission* – (Connecticut) **CFTC says Connecticut resident ran \$5.4M Ponzi scheme.** The U.S. Commodity Futures Trading Commission (CFTC) November 27 announced the filing of a civil enforcement action charging a Branford, Connecticut man with operating a commodity pool Ponzi scheme that solicited approximately \$5.4 million from at least 50 people to invest in a commodity pool named First Financial, LLC. The man allegedly misappropriated at least \$900,000 of pool participants' funds, using the funds to pay personal expenses and purchase gifts. The CFTC complaint also charges him with failing to register as a Commodity Pool Operator (CPO) of First Financial. According to the complaint, from at least January 2007 and continuing until September 13, 2012, the man, in order to entice prospective participants, guaranteed monthly and yearly returns of 1 percent to 15 percent on investments in the pool. Of the \$5.4 million solicited from pool participants, at least \$900,000 was misappropriated, approximately \$1.32 million was lost trading futures in accounts in the name of First Financial, and \$3.17 million was paid out to certain pool participants as fictitious "profits" or returns of principal, according to the complaint. The man allegedly admitted to one pool participant that he was operating a Ponzi scheme. To falsely assure pool participants that their funds were safe in the pool's trading accounts, he allegedly fabricated trading account statements from First Financial and from futures commission merchants.

Source: <http://www.futuresmag.com/2012/11/27/cftc-says-connecticut-resident-ran-54m-ponzi-schem?t=managed-funds>

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

## Transportation Sector

10. *November 28, Oklahoma City Oklahoman* – (Oklahoma) **Oklahoma City school bus accident sends students, bus driver to hospitals.** Police were searching November 27 for a driver who toppled a school bus — injuring the driver and students on their way to school — before fleeing on foot. The small Oklahoma City Public Schools bus bound for North Highland Elementary was going north on Classen Boulevard when the driver of a vehicle ran the stop sign at NW 89 going east and hit the bus. The impact overturned the bus. An Oklahoma City Schools spokeswoman said seven students were on the bus. Four students and the driver were taken from the crash scene to hospitals in good condition, an Emergency Management Services Authority spokeswoman said. The bus driver was treated for neck and back injuries. All those taken to hospitals were treated and released, she said.  
Source: <http://newsok.com/oklahoma-city-school-bus-accident-sends-students-bus-driver-to-hospitals/article/3732444>
11. *November 28, Everett Herald* – (Washington) **No lasting fix likely for slides along railroad.** Although some measures to prevent mudslides along railroad tracks between Everett, Washington and Seattle have been taken they will not be enough to fix the drainage problems on the corridor, according to Washington State officials. Travelers on Sounder commuter and Amtrak passenger trains along the route have been plagued by delays from mudslides for years. Most recently, mudslides resulted in closing the line to passenger service the week of November 18, said a spokesman for Burlington Northern Santa Fe Railway, which owns the tracks. The hillsides along the tracks between Everett and Seattle are the worst slide area for trains in western Washington, a high-speed rail program manager for the State Department of Transportation said. The problem is not just the slopes — it is the runoff from developed areas above the slopes along the route. Sounder, which has experienced low ridership because of parking and other issues as well as mudslides, has had more than 200 trips canceled because of slides since it began running in 2003, according to Sound Transit figures. The railroad requires a 48-hour moratorium on passenger service when tracks are blocked by a mudslide. Eight Sounder trains operate on weekdays between Everett and Seattle, four each way. Six Amtrak trains run on the line every day, three each way.  
Source: <http://www.heraldnet.com/article/20121128/NEWS01/711289932>
12. *November 28, Fleet Owner* – (National) **More fraudulent letters sent to motor carriers.** Another round of fraudulent U.S. Department of Transportation (U.S. DOT) letters dated September 24, 2012 were being distributed — largely by fax — to motor carrier officials attempting to obtain banking information from the targeted carriers, according to the Federal Motor Carrier Safety Administration (FMCSA), Fleet Owner reported November 28. The letters appear to be from the “U.S. Department of Transportation Procurement Office” and are signed by a fictitious name. The individual on the letter is not an employee of U.S. DOT, FMCSA said. This was one of many rounds of the scam where many carriers have received a faxed letter asking recipients to provide bank account information on an “Authorization to Release Financial Information” form. In the recurring identity theft scheme the letters are typically signed by someone claiming to be a “Senior Procurement Officer” at DOT and appear on DOT

letterhead containing a Washington, D.C. address.

Source: <http://fleetowner.com/fleet-management/more-fraudulent-letters-sent-motor-carriers>

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

## **Postal and Shipping Sector**

13. *November 28, Detroit Lakes Tribune* – (Minnesota; Wisconsin) **Two wanted in Fergus Falls mail, identity thefts.** The Detroit Lakes Tribune reported November 28 that, according to a WDAY 6 Fargo news report, law enforcement in Fergus Falls, Minnesota, were looking for two people in connection to stealing mail and using it for identity theft. Police said the two suspects took blank checks and other mail from at least six homes. The two took the checks from credit card mailings and use them to deposit money into their own accounts at Affinity Plus Credit Union. The two then allegedly worked their way down Interstate 94, writing more false checks and stealing more mail in the Anoka area, police said. Police believed the two were somewhere in Wisconsin, passing counterfeit bills. One of the suspects pleaded guilty to 35 counts of mail theft in Becker County in 2006.

Source: <http://www.dl-online.com/event/article/id/71474/group/homepage/>

14. *November 27, KOB5 Medford* – (Oregon) **Mail theft on the rise in Douglas County.** Officials in Douglas County, Oregon, said they are already seeing an increase in mail theft, stating thieves are after gift cards, bank statements, social security numbers, and any other items which would lead to stealing your identity or money, KOB5 Medford reported November 27. Officials warned residents not to place mail in their mailboxes overnight.

Source: <http://www.kob5.com/component/zoo/item/mail-theft-on-the-rise-in-douglas-county.html>

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

## **Agriculture and Food Sector**

Nothing to report

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

## **Water Sector**

15. *November 28, Chicago Tribune* – (Illinois) **Water main break nearly empties Western Springs water tower.** A water main break caused a million-gallon water tower to drain November 27 in Western Springs, Illinois. Village officials did not expect to lift a boil water order until sometime November 28, more than 24 hours after the break caused the water tower in Spring Rock Park to drain to nearly empty. A public works crew was on the site November 27 using a backhoe to dig into the sippy ground to find and repair the break underneath a baseball field south of the tower. The

repair was completed. The chief water operator of the village water plant said an alarm on the tower was supposed to alert police of a break of this type. However, the system did not work, and no one in his department knew of the break until November 27.

Source: [http://www.chicagotribune.com/news/local/suburbs/western\\_springs/ct-met-western-springs-water-main-break-20121128,0,5693802.story](http://www.chicagotribune.com/news/local/suburbs/western_springs/ct-met-western-springs-water-main-break-20121128,0,5693802.story)

16. *November 27, Augusta Chronicle* – (South Carolina; Georgia) **Lake Lanier falling but Thurmond is still lower.** Located on the border of Georgia and South Carolina, Thurmond Lake’s pool level November 27 was 314.83 feet above sea level, or 15.17 feet below full pool – the lowest reading in 2012. The U.S. Army Corps of Engineers predicted Lake Lanier, located near Atlanta, could drop 2 to 3 more feet by December 21, while projections for Thurmond Lake said pool levels would remain stable or drop only a few inches through January 2013. In November, flows from Thurmond to the Savannah River were reduced to slow the lake’s decline. Some downstream users were forced to adapt to lower flows, which required cutbacks in hydropower generation along the Augusta Canal.  
Source: <http://chronicle.augusta.com/news/metro/2012-11-27/lake-lanier-falling-thurmond-still-lower?v=1354037993>
17. *November 27, Honolulu Star-Advertiser* – (Hawaii) **Kauai asks Kalaheo residents to conserve water.** The Kauai Department of Water asked Kalaheo, Hawaii residents to reduce their water use for a two-week period while crews conduct repair and maintenance work on the Kalaheo Nursery tank, The Honolulu Star-Advertiser reported November 27. The work is expected to be completed by December 7. Affected areas include the mauka side of Kaunualii Highway from Wawae to Opu Road including Lae and Puuwai; Kikala and Kuli roads; and side streets off these roads. Residents were asked to refrain from car-washing, reduce outdoor irrigation, and take other steps to conserve water.  
Source: <http://www.staradvertiser.com/news/breaking/181120641.html>
18. *November 27, Bangor Daily News* – (Maine) **Bucksport, DEP enter agreement to resolve town’s waste water violations.** The town of Bucksport, Maine, agreed to build a new waste water treatment facility in an effort to resolve discharge violations, the Bangor Daily News reported November 27. For 27 years, Bucksport operated under a federal waiver which allowed its waste water treatment plant to operate under lower standards than most in the country. The waiver was granted under a provision of the Clean Water Act that allowed small polluters that discharge into marine waters to adhere only to “primary treatment standards.” In April, the Maine Department of Environmental Protection (DEP) granted Bucksport a discharge permit without the waiver, despite the fact that the town’s waste water facility was incapable of the now-required secondary treatment. The town was found in violation of its new permit in April, May, and June, releasing twice the monthly average amount of certain pollutants than are now allowed. In October, Bucksport entered into an agreement with the DEP to upgrade its facility, according to a monthly DEP enforcement report. The agreement allows the town to continue operating in violation of discharge standards as long as it follows a timetable for upgraded waste water treatment practices. Bucksport has 18 months to submit a preliminary design for an upgraded treatment facility or a

replacement.

Source: <http://bangordailynews.com/2012/11/27/news/hancock/bucksport-dep-enter-agreement-to-resolve-towns-waste-water-violations/?ref=latest>

19. *November 27, Dickinson Press* – (North Dakota) **Oil executive pleads not guilty to charges.** An oil executive pleaded not guilty November 26 at the Stark County, North Dakota Courthouse to a felony charge that he threatened area drinking water with his company’s hydraulic fracturing, or “fracking,” wastewater disposal practices. Earlier this year, the North Dakota Attorney General’s Office charged the suspect with a Class C felony, arguing that a company led by him knowingly attempted to deceive Industrial Commission inspectors. The State has alleged that the suspect, president of Executive Drilling LLC at the time of the alleged crime, directed employees of another company to modify their fracking wastewater disposal practices, which are watched closely because of environmental concerns. He directed the injection of salt water used in the fracking process into a well that was not properly insulated from groundwater near the Lodgepole formation in Stark County, according to court documents. It is unknown at this time if drinking water was contaminated from the alleged negligence and any findings related to groundwater testing would not be released until a trial, according to the North Dakota Department of Mineral Resources.

Source: <http://www.thedickinsonpress.com/event/article/id/63338/>

20. *November 27, Massachusetts Republican* – (Massachusetts) **Agawam water line break could take 4 weeks to repair, but service should not be interrupted, officials say.** A break November 26 in a major water main in the Feeding Hills section of Agawam, Massachusetts, could take up to 4 weeks to repair, but water services should remain uninterrupted, according to an official with the Springfield Water and Sewer Commission. An executive director of the commission said November 27 that the break occurred November 26 in a 54-inch-diameter water transmission line on North West Street near East View Drive. Customers experienced low water pressure until the break was isolated and the water main was shut down by Springfield Water and Sewer Commission workers, according to her. However, she said there was no loss of water service because two other major water transmission lines were able to take up the slack. She said there were complaints of discolored water in Agawam as well as in parts of Springfield.

Source:

[http://www.masslive.com/news/index.ssf/2012/11/major\\_water\\_main\\_break\\_in\\_agaw.html](http://www.masslive.com/news/index.ssf/2012/11/major_water_main_break_in_agaw.html)

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

## **Public Health and Healthcare Sector**

21. *November 28, Homeland Security News Wire* – (International) **Pacemakers, other implanted devices, vulnerable to lethal attacks.** IT experts reported security flaws in pacemakers and defibrillators could be putting lives at risk, stating that many devices are not properly secured and therefore are vulnerable to hackers who may want to commit an act that could lead to multiple deaths, Homeland Security reported

November 28. The Sydney Morning Herald reported that a famous hacker hacked into a pacemaker in October at the Breakpoint security conference in Melbourne, Australia, and was able to deliver an 830-volt jolt to a pacemaker by logging into it remotely after hacking the device. He, however, did not reveal which models were vulnerable to hackers. The hack was possible because many implanted medical devices use wireless technology and authentication which uses a name and a password, which is the serial and model number of the device. According to the hacker, most medical devices are designed to be easy to access by a doctor who may need to change something quickly in case of an emergency. The hacker found secret commands that doctors use in order to send a “raw packet” of data over the airwaves to find any pacemaker or defibrillator in a specific range and have it respond with its serial and model number. The information allows a hacker to authenticate a device to receive data and perform commands, meaning they can send a command to jolt the heart of multiple devices and, in some cases, in a range of up to twelve meters. The U.S. Government Accountability Office released a report that highlighted problems with the security of medical devices, and called upon the Food and Drug Administration to ensure devices are secure from these attacks.

Source: <http://www.homelandsecuritynewswire.com/dr20121128-pacemakers-other-implanted-devices-vulnerable-to-lethal-attacks>

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

## **Government Facilities Sector**

22. *November 27, Milwaukee-Wisconsin Journal Sentinel* – (Wisconsin) **County building evacuated because of threat.** A county executive ordered the evacuation of the Marcia P. Cogg's Human Services Building November 27, citing an unspecified public safety concern. A Milwaukee Police spokeswoman said someone made threats by social media “directed at the area of 12th and Vliet.” She said police were looking for a suspect known for similar past threats. An American Federation of State, County, and Municipal Employees union official said the evacuation order was related to a threat made on Facebook against someone at the Cogg's Building. The county has about 200 employees who work in the Cogg's Building and the State has about 400 workers there. Source: <http://www.jsonline.com/news/milwaukee/county-building-evacuated-because-of-threat-037qnl-181057651.html>
23. *November 27, Associated Press* – (Tennessee) **30 Tenn. courthouses receive bomb threats.** Authorities said 30 Tennessee counties received false bomb threats to courthouses or other government buildings November 27, forcing evacuations while authorities conducted searches. A Tennessee Department of Safety and Homeland Security spokeswoman said no explosives were found and no arrests were made. A spokesman for the Tennessee Emergency Management Agency said the threats were made in phone calls to county clerk offices. In Memphis, police said an unknown woman called and said she had information that someone was going to blow up three buildings in the city, including the federal building and a post office. Tennessee became the fourth State in November to deal with widespread bomb hoaxes. Oregon, Nebraska, and Washington all had similar threats reported to courthouses.

Source: [http://www.necn.com/11/27/12/24-Tenn-courthouses-receive-bomb-threats/landing\\_nation.html?&apID=0892ed08ac484c09b1d222334911679c](http://www.necn.com/11/27/12/24-Tenn-courthouses-receive-bomb-threats/landing_nation.html?&apID=0892ed08ac484c09b1d222334911679c)

For another story, see item [10](#)

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

## **Emergency Services Sector**

24. *November 28, Spokane Spokesman-Review* – (Washington) **County 911 system still under repair.** Spokane County, Washington 9-1-1 operators continued to work out of a backup communications center following a November 26 system failure for 9-1-1 and Crime Check, the non-emergency police assistance line. When two backup systems also failed, operators were sent to the county's backup communications center. Callers could not get through to 9-1-1 operators for nearly an hour. Phone technicians from CenturyLink continued work November 27 to fix systems that failed at the main emergency communications center. The CenturyLink marketing development manager said it remains unclear what caused the problem. The director of 9-1-1 Emergency Communications said the primary system was back in operation, but the backup systems at the main communications center were not working. She said operators would continue working at the reserve 9-1-1 center until all the systems are fixed. Source: <http://www.spokesman.com/stories/2012/nov/28/county-911-system-still-under-repair/>

25. *November 27, Associated Press* – (New Mexico) **US Justice launches probe into Albuquerque police.** The U.S. Department of Justice launched an investigation of the Albuquerque, New Mexico Police Department after a string of officer-involved shootings and high-profile abuse cases that allege the use of excessive and deadly force, officials said November 27. The announcement of a civil probe comes months after the police department in New Mexico was the target of protests, lawsuits, and demands for wide-scale agency overhaul from civil rights advocates. The city has seen 25 officer-involved shootings — 17 of them fatal — since 2010. Source: <http://www.ksro.com/news/article.aspx?id=3750456>

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

## **Information Technology Sector**

26. *November 28, Softpedia* – (International) **Fake Angry Birds Star Wars hides Android trojan.** GFI Labs experts have identified an application on a Russian Web site that is promoted as Angry Birds Star Wars, but is actually a piece of malware known as Boxer. Boxer is a threat that has been around for quite some time. It is highly popular among cybercriminals because it helps them make a considerable profit by sending SMSs from the compromised smartphone to premium rate numbers. GFI's VIPRE Mobile detects the threat as Trojan.AndroidOS.Generic.A. Experts advise users to download Android apps only from trusted locations such as Google Play.

Source: <http://news.softpedia.com/news/Fake-Angry-Birds-Star-Wars-Hides-Android-Trojan-310405.shtml>

27. *November 28, Help Net Security* – (International) **Malicious ads lead to fake browser updates.** StopMalvertising warns of an upswing of “Your browser is out of date” trick used to infect computers with malware. The scam starts with malicious ads leading to pages able to detect which browser users use and serve them with a fake notification about them needing to update their browser. The landing page was initially located on securebrowserupdate.com, but has since been removed. These served pages have the look and the feel of the legitimate browsers’ sites they are trying to impersonate. According to Trend Micro, French, U.S., and Spanish users are among the most targeted/gullible. “Instead of an update, users download a malware detected as JS\_DLOADR.AET, which was found capable of changing the downloaded binary to have a different payload,” Trend Micro researchers shared. “The malicious JavaScript, in turn, downloads TROJ\_STARTPA.AET and saves it as {Browser Download Path}\install.exe. Based on our initial analysis, the Trojan modifies the user’s Internet Explorer home page to http://{BLOCKED}rtpage.com, a site that may host other malicious files that can further infect a user’s system.”

Source: [http://www.net-security.org/malware\\_news.php?id=2337&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm\\_content=Google+Reader](http://www.net-security.org/malware_news.php?id=2337&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)

28. *November 27, Help Net Security* – (International) **Hardcoded account in Samsung printers provides backdoor for attackers.** The U.S. Computer Emergency Readiness Team (US-CERT) issued an alert warning users of Samsung printers and some Dell printers manufactured by Samsung about the presence of a hardcoded account that could allow remote attackers to access an affected device with administrative privileges. This privileged access could also be used to change the device configuration, access sensitive information stored on it (credentials, network configuration, etc.), and even to mount additional attacks through arbitrary code execution, US-CERT claims. The hardcoded account is present in all printers released before October 31, 2012. Samsung said that a patch will be pushed out “later this year.”

Source: [http://www.net-security.org/secworld.php?id=14020&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm\\_content=Google+Reader](http://www.net-security.org/secworld.php?id=14020&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)

29. *November 27, Krebs on Security* – (International) **Java zero-day exploit on sale for ‘five digits’.** Miscreants in the cyber underground are selling an exploit for a previously undocumented security hole in Oracle’s Java software that attackers can use to remotely seize control over systems running the program, KrebsOnSecurity has learned. The flaw, currently being sold by an established member of an invite-only Underweb forum, targets an unpatched vulnerability in Java JRE 7 Update 9, the most recent version of Java (the seller says this flaw does not exist in Java 6 or earlier versions). According to the vendor, the weakness resides within the Java class “MidiDevice.Info,” a component of Java that handles audio input and output. “Code

execution is very reliable, worked on all 7 version I tested with Firefox and MSIE on Windows 7,” the seller explained in a sales thread on his exploit. It is not clear whether Chrome also is affected.

Source: [http://krebsonsecurity.com/2012/11/java-zero-day-exploit-on-sale-for-five-digits/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+KrebsOnSecurity+\(Krebs+on+Security\)&utm\\_content=Google+Reader](http://krebsonsecurity.com/2012/11/java-zero-day-exploit-on-sale-for-five-digits/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+KrebsOnSecurity+(Krebs+on+Security)&utm_content=Google+Reader)

For more stories, see items [6](#), [8](#), and [21](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto: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: <https://www.it-isac.org>

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

## Communications Sector

Nothing to report

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

## Commercial Facilities Sector

30. *November 28, KIRO TV 7 Seattle* – (Washington) **23 without homes after Bellevue apartment building burns.** The Red Cross assisted 23 residents with temporary shelter and food following a fire at a three-story apartment building fire in Bellevue, Washington, November 27. Firefighters heard reports of people shouting from the upper windows that they could not get out of the apartments. Firefighters told the media they did not know if the residents were blinded by smoke or too frightened to move, but rescuers were able to get everyone down to the street safely. The first fire crew on the scene took one look at the flames and called for other units to back them up. About 60 people were looking for shelter when the Red Cross arrived.

Source: <http://www.kirotv.com/news/news/bellevue-firefighters-respond-three-story-apartmen/nTHGs/>

31. *November 28, Memphis Commercial Appeal* – (Tennessee) **Early morning fire damages St. William Catholic Church in Millington.** Fire investigators searched through the rubble at St. William Catholic Church in Millington, Tennessee, November 28 to determine the cause of a fire that heavily damaged the church offices. The Millington Fire Chief said when firefighters arrived at the scene and they discovered fire coming through the roof of the office section adjacent to the north end of the sanctuary. The chief said there was some smoke and water damage to the sanctuary, but a firewall separating the church from the office section prevented further damage. He said with daylight, they hoped to determine the cause of the fire, which was under

control in about an hour. Fire departments from Millington, Bartlett, and Shelby County were on the scene to fight the blaze. He said part of the investigation would be contacting Alcohol, Tobacco, and Firearms officials to see if they need to investigate. He said there was no reason to suspect any suspicious activity indicating the church as a target, but such calls were “routine” when a place of worship was involved.

Source: <http://www.commercialappeal.com/news/2012/nov/28/early-morning-fire-damages-st-william-catholic-chu/>

32. *November 27, WTXL 27 Tallahassee* – (Florida) **Careless smoking believed to be the cause of Plantations at Pine Lake fire.** Investigators said they now believe careless smoking was to blame for a November 27 fire at a Tallahassee, Florida apartment complex. A lieutenant with the Tallahassee Fire Department said they were called out to the Plantations at Pine Lake apartment complex and found building 9 already engulfed in flames when crews arrived. The lieutenant said the two-story apartment building contained 16 apartment units, 8 of which are effected by fire and/or water damage. Three of those units were heavily damaged by fire. The American Red Cross assisted 23 people displaced following an early morning apartment fire. They planned to place the residents in hotels and provide other emergency assistance as needed. Early damages were estimated at \$1,000,000.

Source: [http://www.wtxl.com/news/local/careless-smoking-believed-to-be-the-cause-of-plantations-at/article\\_6dd5c664-389d-11e2-87fd-0019bb30f31a.html](http://www.wtxl.com/news/local/careless-smoking-believed-to-be-the-cause-of-plantations-at/article_6dd5c664-389d-11e2-87fd-0019bb30f31a.html)

33. *November 27, The Register* – (Texas) **Hotel blames burglaries on hacked Onity card locks.** A Texas hotel claimed to have suffered multiple burglaries stemming from flaws in a common type of electronic lock, exploits for which were demonstrated at this year’s Black Hat hacking conference, the Register reported November 27. The Hyatt hotel in Houston’s Galleria complex told Forbes that its guests suffered a string of break-ins in September, and that it identified the hacking of its Onity locks as the method used. The suspect was arrested for the break-ins and has helped the police with their inquiries. The hotel owners said they became aware of the issue with Onity locks in August and were working with the company on a fix when the thefts took place. At the time of the Black Hat presentation, Onity called the hack “unreliable, and complex to implement,” but it appears not too complex for others to imitate. So far Onity has offered two workarounds – covering up the data port with screws that are difficult to remove, or replacing the entire circuit board of the lock, which the manufacturer wants hotels to pay for themselves.

Source: [http://www.theregister.co.uk/2012/11/27/hotel\\_onity\\_locks\\_hacked/](http://www.theregister.co.uk/2012/11/27/hotel_onity_locks_hacked/)

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

## **National Monuments and Icons Sector**

34. *November 28, Associated Press* – (Colorado) **Gusts fuel Rocky Mountain National Park wildfire.** Strong gusts and low relative humidities stoked a wildfire burning in Rocky Mountain National Park, Colorado, and prompted the fire’s incident commander to order more resources to contain the flames, the Associated Press reported November 28. The 1,370-acre Fern Lake Fire started October 9. Firefighters have tried to suppress

it, but direct attacks were limited because the fire was burning in steep, rugged terrain, some of which includes trees killed by beetles. The fire was active November 27 due to conditions that were ripe for burning, and sparks from the fire jumped Spruce Creek to the southern side. The incident commander ordered more resources, including a helicopter to fight the flames. The fire was listed at 40 percent contained. The park was open, but trails near the fire are closed

Source: [http://www.sbsun.com/living/ci\\_22080579/gusts-fuel-rocky-mountain-national-park-wildfire](http://www.sbsun.com/living/ci_22080579/gusts-fuel-rocky-mountain-national-park-wildfire)

35. *November 28, WNYW 5 New York* – (New York) **Statue of Liberty, Ellis Island to remain closed through 2012.** The Statue of Liberty and Ellis Island will remain closed through at least the rest of 2012, the National Park Service (NPS) announced November 28. Facilities and infrastructure on both islands, which together make up the Statue of Liberty National Monument, suffered damage in superstorm Sandy's historic storm surge. The Statue of Liberty itself, the pedestal, and the base were unharmed, but the storm chewed up a brick walkway, railings, and docks on Liberty Island. On Ellis Island, the storm damaged exhibits, displaced some fuel oil tanks, beached a U.S. Park Police boat, damaged and uprooted a police trailer, flooded machinery in the basements of the historic hospital and administration buildings, and littered the area with debris. Crews were present to pick up debris on both islands and have started repair work, the NPS said. A NPS spokeswoman said no reopening date had been set and would not be announced until at least January 15, 2013.

Source: <http://www.myfoxny.com/story/20162511/statue-of-liberty-ellis-island-to-remain-closed>

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

## **Dams Sector**

36. *November 27, Associated Press* – (Louisiana) **Big bill for levee upkeep comes to New Orleans.** By the time the next hurricane season starts in June of 2013, New Orleans will take control of much of a revamped protection system of gates, walls, and armored levees that the U.S. Army Corps of Engineers has spent about \$12 billion building, the Associated Press reported November 27. The Corps has about \$1 billion worth of work left. The Corps estimated it would take \$38 million a year to pay for upkeep, maintenance, and operational costs after it was turned over to local officials. At current funding levels, the region will run out of money to properly operate the high-powered system within a decade unless a new revenue source was found. New Orleans voters voted on renewal of a critical levee tax November 6. The tax levy was approved, meaning millions of dollars should be available annually for levee maintenance. After Katrina, the locally run levee boards that oversaw the area's defenses were vilified, and quickly replaced by the regional levee district. However, experts generally agree the old levee board's failings did not cause the levees to collapse during Katrina. The collapse was mainly attributed to poor levee designs by the Corps and the sheer strength of the hurricane.

Source:

[http://www.google.com/hostednews/ap/article/ALeqM5jUrnhBNAQuZHb6MfjbLIagg\\_bLmg?docId=f3cd2896190e466490afd49853240fb0](http://www.google.com/hostednews/ap/article/ALeqM5jUrnhBNAQuZHb6MfjbLIagg_bLmg?docId=f3cd2896190e466490afd49853240fb0)

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



**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](mailto:cikr.productfeedback@hq.dhs.gov) or contact the DHS Daily Report Team at (703)387-2314

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](mailto: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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.