



# Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 03 December 2003

Current Nationwide Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)  
[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- The Boston Herald reports that as the outsourcing of services that involve sensitive data increases, experts warn that private records may be at risk. (See item [6](#))
- Government Executive Magazine reports federal airport screeners argue that a recent drug bust at Kennedy International Airport shows that the use of workers from private companies in sensitive security jobs poses a substantial risk. (See item [7](#))
- eWEEK reports security professionals took note of a critical new vulnerability in the Linux kernel that could enable an attacker to gain root access to a vulnerable machine and take complete control of it. (See item [24](#))

### DHS/IAIP Update *Fast Jump*

**Production Industries:** [Energy](#); [Chemical](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [General](#); [DHS/IAIP Web Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels:** **Physical:** Elevated, **Cyber:** Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *December 01, Associated Press* — **Power outages affect parts of Massachusetts. Power outages swept through Cape Cod and southeastern Massachusetts Monday, December 1.** A spokesperson for utility company NStar did not know what caused the outage and did not know how many people were affected. **A fire at a power plant in Sandwich, MA, may have been connected to the blaze, said a spokesperson for Mirant, which owns the Canal Electric Plant.** "It's not clear at this point whether something triggered the plant to go

offline and caused the fire" or if the fire caused the plant to go offline, said Mirant Spokesperson David Payne. The outages began around 6:15 p.m. Power was being restored to some communities by 7:30 p.m., around the same time that the fire was put out, according to officials.

Source: <http://www.thebostonchannel.com/news/2674752/detail.html>

- December 01, Associated Press* — **Bush signs energy appropriations bill. President Bush on Monday, December 1, signed a \$27.3 billion energy and water bill.** The bill gave Bush most of what he sought for early work on a long-delayed nuclear waste repository at Yucca Mountain, NV. **The legislation, which funds hundreds of water projects from coast to coast, was approved by the House 387-36 and by the Senate on a voice vote.** The energy-water bill approved by the House provided half the \$15 million Bush proposed for research on "bunker buster" bombs, designed to destroy underground targets. It also had all \$6 million he wanted for research into "mini-nukes" of less than 5 kilotons, though the administration will get \$4 million of that amount only after giving lawmakers a report on the status of the nation's nuclear weapons stockpile. **The bill included \$580 million for Yucca Mountain, about 90 miles northwest of Las Vegas, NV.** The legislation funds programs of the Department of Energy, the Department of Interior's Bureau of Reclamation, the Army Corps of Engineers and several other agencies.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A26268-2003Dec 1.html>

- October 30, Government Accounting Office* — **GAO-04-32: Nuclear Regulation: NRC Needs More Effective Analysis to Ensure Accumulation of Funds to Decommission Nuclear Power Plants (Report).** In a report published on Monday, December 1, and dated October 30, the Government Accounting Office (GAO) found that **following the shutdown of a nuclear power plant a significant radioactive waste hazard remains until the waste is removed and the plant site decommissioned.** In 1999, GAO reported that the combined value of the owners' decommissioning funds was insufficient to ensure enough funds would be available for decommissioning. GAO was asked to update its 1999 report and to evaluate the Nuclear Regulatory Commission's (NRC) analysis of the owners' funds and its process for acting on reports that show insufficient funds. **NRC should (1) develop an effective method for determining whether owners are accumulating decommissioning funds at sufficient rates and (2) establish criteria for taking action when it is determined that an owner is not accumulating sufficient funds.** NRC disagreed with these recommendations suggesting that its method is effective and that it is better to deal with unacceptable levels of financial assurance on a case-by-case basis. Highlights: <http://www.gao.gov/highlights/d0432high.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-32>

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

## **Chemical Sector**

Nothing to report.

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

## **Defense Industrial Base Sector**

4. *December 01, Associated Press* — **Air Force pairs veterans with inexperienced fighter pilots. The Air Force is dealing with a training gap by pairing veteran Reserve fighter pilots with less-experienced fliers. While the Air Force needs 330 to 380 new pilots a year, it has the resources to train only 302, a Department of Defense study found. Years of military downsizing and better commercial pilot pay thinned the nation's military aviator ranks.** "Now, we're trying to capture that experience that's walking out the door," Lt. Colonel David "Picker" Cotton said. **Reserve officers like Cotton have been helping close that gap through the Air Force's Fighter Association Program.** Cotton, a Reserve unit commander, and three other Reserve pilots are in the program at Shaw Air Force Base's 55th Fighter Squadron in Sumter, SC. Cotton has more than 2,600 hours flying an F-16. He works in all phases of flying – from mission planning through debriefing – with less experienced pilots like Lt. Ted Schultz, 26, who has just 100 hours. A fighter pilot generally needs 500 flight hours to be considered fully experienced, and the average flying time in an active-duty unit is 600 to 700 hours. The more seasoned pilots "bring an open perspective and they're more approachable," Schultz said.

Source: <http://www.thestate.com/mld/thestate/news/local/7387601.htm>

5. *December 01, Associated Press* — **Navy brig testing biometric tracking. The Navy's Consolidated Brig, which holds some high-profile terrorism suspects, is also testing new monitors which scan inmates' fingers and hands to keep track of the prisoners within the prison.** "There's no place in the country that is applying biometrics like we're doing it in the brig," said Allan Turner, a researcher for the National Institute of Justice, which is working with the brig on the project. **The monitors are being used to track the normal inmate population in the brig.** Most prisons use some sort of paper documentation — paper passes and sign-in sheets — when prisoners move from one area of a prison to another. "Well, you can quickly see that this type of system can be fraught with error," said Turner. For the past four years, researchers have studied different biometric systems to track prisoners. The systems use computers to recognize personal characteristics such as eyes, faces, voices or fingerprints. After researchers studied several technologies, the brig installed 19 monitors that scan inmates' fingers and hands. The next step, Turner said, is to use it in "a more hardened environment like a state prison."

Source: <http://www.thestate.com/mld/thestate/news/local/7387587.htm>

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

## **Banking and Finance Sector**

6. *November 30, Boston Herald (MA)* — **Private records may be at risk. As the outsourcing of services that involve sensitive data increases, experts warn that scandals will increase.** A recent example is when a Pakistani woman, who works in Asia and transcribes medical notes about Americans, threatened to post patients' records on the Internet unless she got a raise. The issue has risen to the political level with one U.S. senator proposing a "Call Center Consumer's Right to Know Act," designed to protect the jobs and privacy of Americans. The back-and-forth flow of data between the United States and foreign work sites is tied to the escalating corporate trend of outsourcing jobs to developing countries. **The outsourcing controversy has mostly focused on the loss of tens of thousands of U.S. high-tech jobs to**

**developing countries. But an increasing number of outsourced jobs also include call-center personnel, accountants, financial analysts, medical assistants and others in posts with access to personal data, from Social Security numbers to bank records.**

Defenders of outsourcing say a combination of U.S. laws and strict security measures by corporations will protect Americans' privacy. But critics say privacy laws in the United States — unlike those in the European Union — have too many legal loopholes that permit the outsourcing of both jobs and data with little built-in protections.

Source: <http://business.bostonherald.com/businessNews/business.bg?articleid=930>

[[Return to top](#)]

## **Transportation Sector**

7. *December 02, Government Executive Magazine* — **Airport drug bust heightens debate over non-federal forces.** A recent drug bust at Kennedy International Airport shows that the use of workers from private companies in sensitive security jobs poses a substantial risk, federal airport screeners argued Monday. **Government agents arrested 20 baggage and cargo handlers at Kennedy last Tuesday and charged them with slipping tens of millions of dollars worth of cocaine and marijuana past security checkpoints during the last decade.** Authorities said the workers were employed by American Airlines, Delta Airlines, United Airlines and five smaller companies: Globe Ground North American, Evergreen Eagle, Hudson General, Swissport USA and Flying Foods. **The operation represented "a potential threat to homeland security," said Michael Garcia, acting head of the Bureau of Immigration and Customs Enforcement.** "A network of corrupt airport employees, motivated by greed, might just as well have been collaborating with terrorists as with drug smugglers," Garcia said following the arrests. Although baggage and cargo handlers must pass background checks, they are not subject to the stringent security checks faced by federal baggage and passenger screeners with the Transportation Security Administration.

Source: <http://www.govexec.com/dailyfed/1203/120103c1.htm>

8. *December 02, WBBM News (Chicago, IL)* — **Metra Rock Island trains affected by freight train derailment.** Crews Tuesday morning were working to right a derailed freight train, blocking tracks shared with Chicago's Metra commuter trains. Metra general road master Al Bobby said the commuter rail service had expected to start moving the derailed cars from the tracks near 1600 S. Clark St. at around 1 a.m. and planned to run the first train through sometime between 5:30 a.m. and 6 a.m. A spokesman for Canadian National, a rail, truck and communications conglomerate, said his organization was pushing for 4 a.m. as the time when the cars could be set back onto the tracks. A crew from the Hulcher company, a heavy-equipment firm, brought cranes to the scene to return the train to the tracks, said the CN spokesman, who did not want his name used. **The train derailed at around 8:45 p.m. Monday, as it was switching to another set of tracks, police News Affairs Officer Carlos Herrera said. Officials did not know the cause of the derailment as of about 11 p.m. Monday, according the CN spokesman.** A foam truck was sent as a precaution, but there was no fire and a test for hazardous materials was negative.

Source: <http://www.wbbm780.com/asp/ViewMoreDetails.asp?ID=31229>

9.

*December 01, New York Post* — **Bomb threat grounds plane.** A plane bound for Newark was detained in San Francisco after someone phoned in a bomb threat to the airport, San Francisco airport police said early Monday morning. **The caller warned a bomb would explode aboard ATA flight 618 at about 1 a.m eastern time, cops said. The flight was scheduled to take off about an hour earlier. All 227 passengers were removed from the plane and were re-screened as was all the luggage on board.** Although the callers' deadline passed, the search of the plane continued early this morning, but police believed the threat was a hoax. Source: <http://www.nypost.com/news/nationalnews/12266.htm>

10. *December 01, Transportation Security Administration* — **TSA outlines security recommendations for general aviation.** A coalition of general aviation associations established as a working group of the Transportation Security Administration's (TSA) Aviation Security Advisory Committee has delivered a series of recommendations for enhancing security at general aviation airports, including tighter identification of passengers flying on private planes, closer monitoring of student pilots, and improving airport surveillance. "Since 9/11, general aviation has worked closely with TSA to voluntarily enhance security at facilities across the country," said Stephen McHale, TSA Deputy Administrator, who met with top representatives of 17 general aviation associations to discuss the recommendations. **TSA will build on these recommendations to establish formal guidelines that general aviation airports can follow to further strengthen security. By early next year, TSA will issue "best practice" guidelines for security at more than 18,000 landing facilities nationwide that serve general aviation.** Many of the airports, which serve more than 275,000 general aviation aircraft, already have implemented at least some of the working group's recommendations, while the TSA and other government agencies also have moved to tighten general aviation security. Source: [http://www.tsa.gov/public/display?theme=44&content=090005198\\_006ed9a](http://www.tsa.gov/public/display?theme=44&content=090005198_006ed9a)

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

## **Postal and Shipping Sector**

11. *December 02, DM News* — **Carrier pickup service.** The U.S. Postal Service (USPS) is testing a new service called Carrier Pickup that lets customers request next-day package pickups, the agency said Monday. Customers make the request through a special Web site. The local post office retrieves that information, and letter carriers are notified of any pickup requests before they begin their routes the next day. There is no pickup fee, because the packages are picked up from the customers as part of the carrier's normal delivery route. Carrier Pickup is being tested at post offices in Arizona, New York on Long Island, and in California in Los Angeles, San Diego, Van Nuys, and Santa Ana. **National rollout could begin as early as January.** Source: [http://www.dmnews.com/cgi-bin/artprevbot.cgi?article\\_id=2577\\_0](http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=2577_0)

12. *December 02, Associated Press* — **Postal Service expects heavy shipping traffic. An improving economy means the U.S. Postal Service will handle 20 billion letters and packages this holiday season.** "Generally that economic news translates into additional volume for us," Chief Operating Officer Patrick Donahoe said. Donahoe said they already have seen a one percent increase in volume compared to the 2002 holiday season, and he expects that

to go higher. The heaviest mailing day should be December 15, with 850 million to 900 million cards and letters going out. **Air cargo capacity will be increased by nearly 40 percent two weeks before Christmas, and hundreds of trucks will be added.** The Postal Service plans to hire only 10,000 temporary employees, half as many as last season, officials said. UPS and FedEx are making similar preparations. To ship an estimated 300 million packages, UPS scheduled additional and late pickups for peak days. **UPS is also adding nearly a dozen large jets to its air fleet, and will hire more than 50,000 temporary employees. FedEx expects its average daily package volume to increase by around 20 percent and plans to hire several thousand people to help with the additional load.** On its busiest day, December 15, the company expects to handle around seven million packages.

Source: <http://www.marini.com/Stories/0.1413.234~26641~1804047.00.html>

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

## **Agriculture Sector**

13. *December 02, Associated Press* — **Tree beetle found in central Ohio. A beetle that has destroyed millions of ash trees in Michigan has been found for the first time in a handful of trees in Central Ohio.** Until now, the beetle had been in Ohio only in the northwest corner. At least eight trees showed signs of being infested near a Columbus auto–repair shop, according to the Ohio Department of Agriculture. They were planted two years and brought to Ohio from a nursery in Michigan where the emerald ash borer beetle was discovered last year. The beetle has infested or destroyed about six million ash trees in southeast Michigan, mostly near Detroit. It also has been found in northwest Ohio and in Maryland. Inspectors discovered the infestation on the northwest side of Columbus after investigators traced a shipment of ash trees from the Michigan nursery to a Columbus landscaping company. The trees were sold in 2001, two years before Ohio prohibited the shipment of ash trees and lumber from Michigan. **Inspectors visited seven sites where the trees were planted to look for larvae. The other sites appeared to be clean. It's not known whether the beetle was able to spread in the area.**

Source: <http://www.nbc4columbus.com/news/2673872/detail.html>

14. *December 02, Agricultural Research Service* — **Boosting potatoes' natural ability to protect themselves.** Potato and other plants have the means to defend themselves from insects and microbes that cause disease. But some plants don't mobilize these defenses in time to do much good. Agricultural Research Service (ARS) scientists are testing a way to snap plants to attention and steel them for battle. **In studies, the scientists are spraying the plants with salicylic acid. In plants, it functions as a natural signaling compound that triggers a protective response called "systemic acquired resistance," (SAR).** Plant scientists have known about SAR for years, but only recently have SAR–activating products become available for use on crops including tomatoes, lettuce, and spinach. **Healthier plants and reduced pesticide use are among the benefits associated with activating SAR.** But according to Roy Navarre, a molecular biologist at ARS, little is known about such benefits in potatoes, a crop that generates nearly \$3 billion annually in the U.S. So, earlier this year, he and colleagues kicked off a project to find out. Through lab and field studies, their objective is to determine which SAR activators work best, in what parts of the potato plant, for how long and at what doses.

Source: <http://www.ars.usda.gov/is/pr/2003/031202.htm>

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

## **Food Sector**

Nothing to report.

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

## **Water Sector**

15. *December 02, KATU News* — **Arsenic worries Oregon water testing.** A dangerous chemical in their drinking water has been facing homeowners in part of northwest Clark County, OR. **Health officials are trying to figure out if arsenic is making people sick. What makes this case more confusing to trace, is a cluster of people in the area with a rare disease called Guillain–Barré syndrome.** Symptoms of the syndrome include numbness in the legs, spreading to the arms and upper body. In severe cases it can lead to paralysis. **The symptoms of Guillain–Barré are also seen in arsenic poisonings.** So far state health officials don't think there's a connection. The county is urging homeowners who received letters to have their water tested. Homeowners are hoping the county will bring in piped water in the next couple years.

Source: <http://www.katu.com/news/story.asp?ID=62847>

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

## **Public Health Sector**

16. *December 01, Reuters* — **SARS vaccine. Canadian researchers are immunizing ferrets with three different test vaccines in a fast–tracked effort to find a way to ward off the Severe Acute Respiratory Syndrome (SARS) virus,** researchers told a symposium on Monday. Research funded by the province of British Columbia could see human trials in place as early as next fall if there was another SARS outbreak. **It's part of an experimental approach to apply research more rapidly to health emergencies,** said Brett Finlay, a microbiologist from the University of British Columbia, who is leading the project. In an environment where it can take a year to approve a project, Finlay's team aimed to grant funding in 24 hours, he said. This is not how you want to do all science, but I think for an emerging infectious disease as it's racing around the world, I think we have to have these mechanisms in place," he said. If the vaccines work for ferrets, which are susceptible to SARS, the researchers will next test the vaccines on primates, and then humans, he said.

Source: <http://www.alertnet.org/thenews/newsdesk/N01215224.htm>

17. *December 01, Associated Press* — **Scientists get images of West Nile virus.** The first high–resolution images of the West Nile virus reveal a tiny microorganism that looks something like a bumpy gum ball. **The three–dimensional images obtained by Purdue University researchers give scientists their most detailed look yet of the virus and could help them design drugs to disarm it.** Richard J. Kuhn, a professor of biological sciences in Purdue's School of Science, said his team's images show that the West Nile virus is different

from irregularly shaped viruses such as influenza or measles. The surfaces of those viruses have proteins that project away in arm-like appendages they use to latch onto receptors on cells that they then hijack, infect, and use to reproduce. By contrast, the West Nile virus is spherical with surface proteins folded into an interlocking pattern. Understanding the precise orientation of those proteins the Purdue team's next goal could speed the development of drugs to thwart its ability to infect cells in birds, humans, horses and other animals. **A West Nile vaccine has been developed for horses, but none currently exists for humans.**

Source: [http://abcnews.go.com/wire/Living/ap20031201\\_808.html](http://abcnews.go.com/wire/Living/ap20031201_808.html)

18. *December 01, Knight Ridder Newspapers* — **Stomach virus sickens cruise passengers. More than six dozen passengers on the Carnival Cruise Lines' Legend's Caribbean trip were stricken with a stomach illness last week. The previous Legend cruise had even more sick guests. The illness was believed to have caused by norovirus, according to public health officials.** On this trip, just over three percent, or 73 out of 2,378 passengers on board, reported similar symptoms, according to the Centers for Disease Control and Prevention (CDC). Four of 913 crew members were also affected. "It's an outbreak by definition," said David Forney, chief of vessel sanitation for the CDC, who cautioned that the virus was an extremely common one, afflicting 23 million people a year. Forney said Carnival was doing "everything they can and everything we ask" to deal with the outbreak. **In the past year, the norovirus, also called the Norwalk virus, struck more than 1,500 passengers on cruise ships sailing from ports on both U.S. coasts.**

Source: <http://www.bayarea.com/mld/cctimes/news/7386000.htm>

[[Return to top](#)]

## Government Sector

19. *December 02, Contra Costa Times (California)* — **California assembly repeals controversial driver's license bill.** As the California state Assembly voted Monday to repeal a controversial law allowing illegal immigrants to obtain driver's licenses, Gov. Arnold Schwarzenegger and key Democrats pledged to work together on a new version that addresses national security concerns. **They said they would look at possible requirements that undocumented license applicants undergo background checks or apply for legal U.S. residency.** Some lawmakers have criticized the law, SB60, which former Gov. Gray Davis signed in September, **for opening the state's licenses to forgery and for giving driving privileges to people living illegally in the country. The law, which would have taken effect next month, would have allowed an estimated two million illegal immigrants to submit federally issued taxpayer identification numbers instead of Social Security numbers to apply for a license.**

Source: <http://www.bayarea.com/mld/cctimes/news/state/7393314.htm>

20. *December 02, PHXnews.com (Phoenix, AZ)* — **Homeland Security Secretary Tom Ridge will join Sen John McCain on aerial border tour.** U.S. Senator John McCain (R-AZ) announced today that Homeland Security Secretary Tom Ridge will join him in Arizona on Wednesday to assess various Arizona border issues. **They will travel to Ft. Huachuca to see a demonstration of the use of Unmanned Aerial Vehicle's (UAV's).** Border security officials are investigating the possibility of deploying UAV's along the U.S. – Mexico border as a means of improving border security. Following the demonstration at Ft. Huachuca, Secretary Ridge

and Senator McCain will take an aerial border tour of the Arizona – Mexico border. "I am pleased Secretary Ridge will be visiting the Arizona border. With this trip the Secretary will be able to see first hand the border problems confronting Arizonans. I look forward to working with him to reform our immigration policy," McCain said.

Source: <http://www.phxnews.com/fullstory.php?article=7840>

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

## **Emergency Services Sector**

21. *December 02, Federal Computer Week* — **USC to study terrorism and economics.** The University of Southern California (USC) will receive \$12 million in federal funding over the next three years to study economic risks from potential terrorist threats and events to targets, such as critical infrastructure systems, and develop tools for planning responses and emergencies. USC becomes the first Center for Excellence under a Homeland Security Department program to enhance multidisciplinary academic research to enhance prevention, response and recovery from terrorism events. Specifically, USC will establish the Homeland Security Center for Risk and Economic Analysis of Terrorism Events. **The center will offer courses and a certificate program in risk and decision analysis to distance-learning engineering students and develop professional workshops, fellowships and outreach to local and regional communities, among other research activities.** Two existing USC centers — the Integrated Media Systems Center and Information Sciences Institute — will contribute research in advanced computer modeling and cybersecurity.

Source: <http://fcw.com/geb/articles/2003/1201/web-usc-12-01-03.asp>

22. *December 02, Ahwatukee Foothills News (Arizona)* — **Emergency telephone notification system gets final test.** This week a computerized emergency notification system for Maricopa County will get its final test before becoming operational January 1, 2004. **Designed to alert residents during an emergency, the Community Emergency Notification System uses the existing 911 database to make as many as 2,200 telephone calls a minute, according to the Maricopa Association of Governments (MAG).** The \$2.5 million system can inform residents of emergencies such as fires, toxic chemical spills, floods or police incidents. The message can also provide instructions in English or Spanish on what actions to take, including providing evacuation directions.

Source: <http://www.ahwatukee.com/afn/community/articles/031203a.html>

23. *December 01, Washington Post* — **Storm KO'd Virginia's disaster plan.** Virginia's top emergency official said Monday that a computer designed to track requests for help from local governments failed repeatedly during Hurricane Isabel, delaying the distribution of ice, water, generators and other assistance. **Michael Cline, the director of the state's Department of Emergency Management, told lawmakers at a hearing that the state's "Action Tracking" computer system did not have a battery backup. When the power went out, requests for help were lost.** "There were a lot of breakdowns in communications," Cline told members of the Senate and House commerce committees. "We are trying to work with each of those local governments. Communication was obviously a major issue." In the days after the storm swept across Virginia, officials in Hampton Roads and other parts of the state complained that their pleas for assistance were going unheeded. Some blamed the Federal Emergency Management

Agency, while others pointed to problems in the state's emergency operations center. Cline said that some state workers were not trained properly and did not know how to use the computer system when it was operational. And he said some requests for help that were entered into the tracking system languished there for days.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A26820-2003Dec 1.html>

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

## Information and Telecommunications Sector

**24. December 01, eWEEK — Researchers find serious vulnerability in Linux kernel.** Security professionals took note of a critical new vulnerability in the Linux kernel that could enable an attacker to gain root access to a vulnerable machine and take complete control of it. An unknown hacker recently used this weakness to compromise several of the Debian Project's servers, which led to the discovery of the new vulnerability. **This discovery has broad implications for the Linux community. Because the flaw is in the Linux kernel itself, the problem affects virtually every distribution of the operating system and several vendors have confirmed that their products are vulnerable.** The vulnerability is in all releases of the kernel from Version 2.4.0 through 2.5.69, but has been fixed in Releases 2.4.23-pre7 and 2.6.0-test6. RedHat Inc. and the Debian Project have both released advisories warning customers of the issue and providing information on fixes. Products from other vendors, including, MandrakeSoft S.A., SuSE Linux AG and Caldera International Inc., are also vulnerable.

Source: <http://www.eweek.com/article2/0.4149.1400446.00.asp>

### Internet Alert Dashboard

| Current Alert Levels   |  |
|--|--|
| <br>AlertCon: 1 out of 4<br><a href="https://gtoc.iss.net">https://gtoc.iss.net</a> | <br>Security Focus ThreatCon: 1 out of 4<br><a href="http://analyzer.securityfocus.com/">http://analyzer.securityfocus.com/</a>  |
| Current Virus and Port Attacks   |  |
| <b>Virus:</b>  | #1 Virus in the United States: <b>WORM_LOVGATE.F</b><br>Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center<br>[Infected Computers, North America, Past 24 hours, #1 in United States]                     |
| <b>Top 10 Target Ports</b>   | 445 (microsoft-ds), 80 (www), 135 (epmap), 137 (netbios-ns), 1434 (ms-sql-m), 17300 (Kuang2TheVirus), 139 (netbios-ssn), 1433 (ms-sql-s), 38293 (NortonAntiVirus), 898 (----)<br>Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center |

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

## General Sector

25. *December 02, Reuters* — **U.S. warns of terrorist threat in Kenyan capital.** The United States warned in a statement Tuesday, December 2, of terrorist threats against Western interests in the Kenyan capital, advising its citizens to stay away from downtown Nairobi in the next few days. **The warning comes ahead of a visit by U.S. Health Secretary Tommy Thompson to Nairobi later this week. The statement said the information had not been corroborated.** The United States already maintains a high level threat warning on travel to Kenya and had issued specific warnings about security threats several times in the past. The U.S. embassy in Nairobi was bombed in 1998, killing 214 people and last November suicide bombers blew up an Israeli-owned hotel near the resort town of Mombasa.

Source: [http://story.news.yahoo.com/news?tmpl=story&cid=578&e=2&u=/nm/20031202/ts\\_nm/security\\_kenya\\_alert\\_dc](http://story.news.yahoo.com/news?tmpl=story&cid=578&e=2&u=/nm/20031202/ts_nm/security_kenya_alert_dc)

26. *December 02, Reuters* — **U.S. embassy warns of possible attacks in Saudi Arabia.** The U.S. embassy in Saudi Arabia warned its citizens on Tuesday, December 2, of possible attacks on compounds housing Westerners, saying it had information that at least one residential complex was under surveillance by militants. In response to the information, the embassy said it was restricting its American employees and their dependants from visiting housing compounds in the capital Riyadh at night. **The U.S. warning comes three days after Britain reminded its 30,000 nationals in Saudi Arabia that militants might be in the final phases of planning attacks in the kingdom.** Last month, two Saudi suicide bombers killed at least 18 people, mainly Arab expatriates, at a Riyadh housing compound. On May 12, the triple suicide bombing of three other housing complexes killed at least 35 people. Saudi authorities have blamed Saudi-born Osama bin Laden's al Qaeda network for both attacks and the recent surge in militant-related violence in the kingdom. **Authorities said last week they had foiled an even bigger attack in Riyadh when security forces found a car primed with over 1.2 tons of explosives. Another 1.3 tons of explosive were found nearby.**

Source: [http://story.news.yahoo.com/news?tmpl=story&cid=564&ncid=716&e=13&u=/nm/20031202/ts\\_nm/security\\_saudi\\_usa\\_dc](http://story.news.yahoo.com/news?tmpl=story&cid=564&ncid=716&e=13&u=/nm/20031202/ts_nm/security_saudi_usa_dc)

27. *December 02, Associated Press* — **U.S. woman gets three years for plot to aid Taliban.** The only woman among a group of American Muslims who tried to ally themselves with the Taliban was sentenced Monday, December 1, to three years in prison. **October Martinique Lewis, 26, was convicted of wiring money to her husband and six other men who tried to cross into Afghanistan in 2001 to aid the Taliban in its fight against U.S. soldiers.** Assistant U.S. Attorney Charles F. Gorder Jr. said the sentence reflects Lewis's cooperation in the case. Last week, Lewis's former husband, Jeffrey Leon Battle, and another man were sentenced to 18 years for conspiracy to levy war against the United States. The group never entered Afghanistan.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A26639-2003Dec 1.html>

28. *December 02, Associated Press* — **UK detains 14 under Terrorism Act.** British police arrested 14 people on suspicion of terrorism offenses in raids around the country Tuesday. Four men were arrested in London on Tuesday morning, and four men and two women were arrested in the university city of Cambridge, London's Metropolitan Police said. West Midlands police said they arrested four men under the Terrorism Act in Dudley and Walsall near Birmingham.

**There were no details released on those arrests, except that police said they were not related to other recent arrests. Those arrested in Cambridge and the four in London were all detained under section 41 of the Terrorism Act “on suspicion of involvement in the commission, preparation, or instigation of acts of terrorism,” police said.**

Source: <http://www.msnbc.com/news/1000178.asp?0cv=NB10>

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

## **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions: [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at 703-883-6631

Subscription and Distribution Information: Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at 703-883-6631 for more information.

### **Contact DHS/IAIP**

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call 202-323-3204.

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.