



# Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 10 March 2004

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

- KLAS TV reports the U.S. Postal Inspection Service says mail fraud is on the rise, and community mailboxes are a big target. (See item [12](#))
- eSecurity Planet reports that according to an advisory from computer security consultants iSEC Security Research, a flaw was found in the Linux kernel memory management code and is completely unrelated to a similar vulnerability reported in February; this flaw carries a "critical" rating. (See item [23](#))
- Microsoft has released "Security Bulletin MS04-009: Vulnerability in Microsoft Outlook Could Allow Code Execution (Important)," and a patch is available on the Microsoft Website. (See item [25](#))

### 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. *March 09, Associated Press* — State seeks to delay new power system. In Wisconsin, the governor, business leaders and consumer groups are urging federal regulators to delay a plan designed to improve the transmission of electricity in the Midwest. They say it would place an unneeded financial burden on consumers and could cripple the state's economy. Opponents of the proposal from the Midwest Independent Transmission System Operator

(ISO) argue it would mean \$200 million a year in additional electric costs in Wisconsin because it is designed to increase prices in areas where transmission is deemed inadequate. Midwest ISO officials say the plan would improve transmission of electricity among utilities and show states where they need to improve generation or transmission.

The Indiana-based nonprofit organization manages transmission operations in all or parts of 15 states and Canada. Midwest ISO believes its wholesale market, once in place, would lower electricity rates overall. It expects to file its application March 31, with the goal of implementing the changes by December 1.

Source: [http://www.wisinfo.com/postcrescent/news/archive/local\\_15114\\_548.shtml](http://www.wisinfo.com/postcrescent/news/archive/local_15114_548.shtml)

2. *March 09, Reuters* — **Strike halts LNG exports. Exports from Trinidad's Atlantic LNG project, the top supplier of liquefied natural gas to the United States, have been shut down by a labor strike by workers from two contracting companies.** "We are unable to supply gas, according to our contracts," Esther Le Gendre, Atlantic's manager of government and public affairs, said on Tuesday, March 9. Four tankers remained out at sea as tugboat operators who assist them in receiving LNG for export markets joined construction workers on Monday, March 8, in protest action, demanding increased wages. U.S. natural gas traders said they believed prices were unlikely to soar because LNG plays a tiny role in the overall U.S. gas market. **"If the strike persists the loss of Trinidad to the U.S. market would be equivalent to about 2 percent of demand in March,"** Ira Joseph, Director of Global LNG at Pira Energy Group said. "The loss more greatly affects the (U.S.) Northeast markets as most of the LNG this winter has been going to Everett (LNG terminal in Massachusetts) and Cove Point (in Maryland)," Joseph added.

Source: [http://hsweb01.screamingmedia.com/PMA/pma\\_newsarticle1\\_reuters.htm?SMDOCID=reuters\\_pma\\_2004\\_03\\_09\\_eng-reuters\\_pma\\_STRIKE-AT-TRINIDAD-ATLANTIC-LNG-HALTS-EXPORTS&SMContentSet=0](http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2004_03_09_eng-reuters_pma_STRIKE-AT-TRINIDAD-ATLANTIC-LNG-HALTS-EXPORTS&SMContentSet=0)

3. *March 09, Dow Jones Newswires* — **Natural gas demand increasing in 2004. Natural gas demand for 2004 is expected to increase by about 2.6% due to anticipated growth in the economy, along with a somewhat lower projected annual average natural gas price, the Energy Information Administration (EIA) said** in its March short-term report issued Tuesday, March 9. Also, the EIA said **underground storage facilities reported above-average withdrawals for February, leaving gas inventories at the beginning of March about 13% below the 5-year average.** Natural gas demand in 2005 is expected to increase by 0.4% as the economy continues to expand. Also, gas production is estimated to have increased approximately 2.2% in 2003. In the electric power sector, demand this year is expected to grow by 2%, the EIA says, driven by accelerated growth in the economy and weather-related increases in the first and the fourth quarters. Next year, annual electricity demand is projected to grow by about 1.8%, as the economic expansion continues. Also, U.S. coal production is expected to increase by 3.6% and 1.3% respectively in 2004 and 2005, as demand for coal increases, the EIA said.

Source: [http://www.quicken.com/investments/news\\_center/story/?story=NewsStory/dowJones/20040309/ON200403091252000746.var&column=P0DEC](http://www.quicken.com/investments/news_center/story/?story=NewsStory/dowJones/20040309/ON200403091252000746.var&column=P0DEC)

4. *March 09, California Independent System Operator* — **Customers lose power after southern California transmission line overloads.** The California Independent System Operator (California ISO) issued a Transmission Emergency at 6:22 p.m. Monday, March 8, after power

lines in the central portion of the state overloaded. ISO operators gave instructions to Southern California Edison (SCE) to "shed load" or rotate customers off the grid for 20 minutes between about 6:30 and 6:50 p.m. **The power outage affected about 70,000 SCE customers. The emergency came after warmer than anticipated temperatures caused a spike in electricity demand in Southern California.** The ISO had anticipated the higher demand for electricity and many power plants were ordered on to meet this first high electrical load of the year. The units were in the process of "ramping up" output, when demand outpaced their ability to generate and keep Path 26 from overloading.

Source: <http://www.caiso.com/docs/2004/03/08/2004030821014911349.pdf>

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

## **Chemical Sector**

5. *March 09, Click On Detroit* — **Hazmat crews head to Detroit chemical plant fire.** Environmental agencies and the U.S. Coast Guard are reportedly on alert as firefighters extinguish a two-alarm fire at a chemical plant in Detroit, Tuesday, March 9. **The Petro-Chem Processing Group plant is located on Lycaste Street on the city's east side,** just east of the Belle Isle Bridge. The plant was reportedly evacuated; however, there were no neighborhood evacuations. Firefighters at the scene were focusing on the second level of the plant, Local 4 News reported. Smoke was still seen coming from the building, but the fire was believed to be under control. Local 4's Steve Garagiola reported a strong chemical odor at the scene during his report. Although hazmat crews were called to the scene, the firefighters were not wearing any type of gas masks, implying there were no hazardous chemicals in the air, the station reported. The U.S. Coast Guard station at Belle Isle and the Marine Safety Office are monitoring the situation, according to Coast Guard officials.

Source: <http://cms.firehouse.com/content/article/article.jsp?id=sectionId=46&id=27279>

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

## **Defense Industrial Base Sector**

6. *March 08, Federal Computer Week* — **Air Force to update electronic warfare database.** The Air Force late last week awarded a \$5.6 million contract to a private contractor to build the Next Generation Electronic Warfare Integrated Reprogramming Database (EWIRDB) system. The contractor's Information Technology division will define, develop and replace the existing EWIRDB system. **EWIRDB combines databases from the National Security Agency, the Defense Intelligence Agency and service intelligence departments.** Electronic warfare is part of the newer, broader information operations capability that uses computer code and radio frequencies to jam or destroy enemy radar and communications networks.

Source: <http://www.fcw.com/fcw/articles/2004/0308/web-airforce-03-08-04.asp>

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

## **Banking and Finance Sector**

7. *March 09, Associated Press* — **World banks work to stop counterfeiting. The world's major central banks confirmed Tuesday, March 9, that they collaborated with leading hardware and software companies to keep personal computers from being used to make counterfeit money.** Work begun nearly four years ago by the Group of Ten central banks resulted in the "counterfeit deterrence system," according to the statement from the Bank for International Settlements (BIS) in Basel, Switzerland. "Several leading personal computer hardware and software manufacturers have voluntarily adopted the system in recognition of the harm that counterfeit currency can cause their customers and the general public," said BIS, known as "the central bankers' central bank." The bank statement said no one could use the technology to track the use of a personal computer or digital imaging tool.  
Source: <http://www.washingtonpost.com/wp-dyn/articles/A43052-2004Mar 9.html>

[[Return to top](#)]

## **Transportation Sector**

8. *March 09, Milwaukee Journal Sentinel* — **First-class cabin the latest place for airlines to compete.** A new battle for the frequent business traveler is starting — and it's taking place at the front of the cabin. Previous battles have focused on fares, frequent-flier miles and even legroom. **Now the low-cost airlines are seeking to steal prized first-class passengers from the traditional carriers. Indianapolis-based American Trans Air, otherwise known as ATA, said it plans to add 12 business-class seats to its planes by November. America West Airlines last month slashed its first-class fares by as much as 70%. And Miami-based Spirit Airlines said it is upgrading its first-class cabin as part of the airline's \$120 million fleet-modernization plan, which it announced last month.** ATA spokesperson Lisa Jacobson Brown said a recent survey of its passengers revealed that the primary perk travelers craved was a first-class cabin. A first-class seat will be priced no more than \$100 above a coach ticket each way, she said. The two largest low-cost carriers, Southwest and JetBlue, said they have no plans to add an elite section. But Southwest is "studying" the cost of adding satellite TV to each of its coach seats, providing a service similar to that of JetBlue Airways, said Southwest spokesperson Ed Stewart.  
Source: [http://cnni.wyellowbrix.com/pages/cnniw/Story.nsp?story\\_id=48144154&ID=cnniw&scategory=Aviation:Airfares&](http://cnni.wyellowbrix.com/pages/cnniw/Story.nsp?story_id=48144154&ID=cnniw&scategory=Aviation:Airfares&)
9. *March 09, The Trucker* — **NATSO looks at fingerprinting Hazmat drivers at truck stops.** Hazmat haulers could be fingerprinted at selected truck stops across the country, if a proposed program by Natso is implemented. **William Fay, president and CEO of NATSO — the National association of travel plazas and truckstops — has been meeting regularly with TSA (Transportation Security Administration) leadership and trucking association executives about this issue.** TSA had set an April 1 deadline to have a Hazmat fingerprint program in place, but the agency has not said if it will meet that deadline. Fay said NATSO's participation would be a way to let Hazmat drivers get the process done the most convenient way possible — while they're at a stop they'd make anyway to fuel up, rest, shower or eat. NATSO also has been talking with representatives of the National Air Transport Association (NATA), which Fay said has fingerprinted about 17,000 of the 30,000 employees who work at airports. Air transportation employees who were fingerprinted were each charged \$72; it's assumed at this point that truckers might be charged close to that amount, said Fay.

Source: [http://www.thetrucker.com/stories/03\\_04/0309\\_fingerprinting.html](http://www.thetrucker.com/stories/03_04/0309_fingerprinting.html)

10. *March 09, Bloomberg* — **EU rejects U.S. aviation deal, will press for broader agreement.** The European Union said a U.S. offer to open up the \$18 billion trans-Atlantic airline market was inadequate and pledged to seek a broader accord. The move comes a week after U.S. Transportation Secretary Norman Mineta said he wouldn't consider letting European airlines, such as British Airways Plc and Deutsche Lufthansa AG, compete on domestic routes. An EU-U.S. aviation accord would encourage airline mergers by at least removing nationality-based traffic-right restrictions in existing U.S. treaties with European countries. The restrictions, which prevent a German airline from flying to the U.S. from Italy, for example, breach rules making the 15-nation EU a single economic area, the bloc's top court has ruled. **Current agreements allow U.S. carriers to load passengers in one EU nation and carry them to another European country. European carriers don't have similar rights in the U.S. market. The EU ultimately wants an agreement that would let European carriers load passengers in U.S. cities and carry them not only to other American destinations but also to third countries such as Mexico.**

Source: <http://quote.bloomberg.com/apps/news?pid=10000085&sid=aLqZaj8xHT7c&refer=europe>

11. *March 09, General Accounting Office* — **GAO-04-380: Contract Management: Coast Guard's Deepwater Program Needs Increased Attention to Management and Contractor Oversight (Report).** The Coast Guard's Deepwater program, the largest acquisition program in its history, involves modernizing or replacing ships, aircraft, and communications equipment. The Coast Guard awarded the Deepwater contract to Integrated Coast Guard Systems (ICGS) in June 2002. The Coast Guard estimates the program will cost \$17 billion over a 30-year period. ICGS is a system integrator, with responsibility for identifying and delivering an integrated system of assets to meet the Coast Guard's missions. The General Accounting Office (GAO) was asked to assess whether the Coast Guard is effectively managing the Deepwater program and overseeing the contractor and to assess the implications of using the Deepwater contracting model on opportunities for competition. **GAO recommends that the Secretary of Homeland Security direct the Commandant of the Coast Guard to take a number of actions to improve Deepwater management and contractor oversight.** Highlights:

<http://www.gao.gov/highlights/d04380high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-380>

[[Return to top](#)]

## **Postal and Shipping Sector**

12. *March 08, KLAS TV (Las Vegas, NV)* — **Mail fraud on the rise.** The U.S. Postal Inspection Service says it might be time to re-think how you pay your bills, especially for people who drop their checks in community mailboxes. The boxes were designed to make it easier on the postal service, and allow neighbors to go to one spot to retrieve their mail. **But the community mailbox, which usually stores anywhere from 6 to 12 mailboxes, has become a popular place for crime. When residents place their checks in the outgoing mail slot, thieves are coming by and collecting them before a mail carrier gets to the box.** It's become such a popular crime, that one U.S. Postal Inspector advises that no money should ever be placed in

these drop slots, especially overnight. "What we don't want people to do is to go out on Saturday night, or whatever night of the week it is, and put it out there and leave that mail out there overnight. If people can keep that mail out of there on an overnight status, they're not going to become a victim," says inspector D. Obritsch. He says the chance of someone stealing your check is decreased just by placing it in the box during the day before a mail carrier comes by.

Source: [http://www.klas-tv.com/Global/story.asp?S=1696859&nav=168XLN\\_w3](http://www.klas-tv.com/Global/story.asp?S=1696859&nav=168XLN_w3)

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

## **Agriculture Sector**

13. *March 10, ABC Radio Australia* — **Taiwan reports outbreak of bird flu. Taiwan has reported a new outbreak of a less virulent form of bird flu and plans to slaughter 12,000 chickens to curb its spread.** The Bureau of Animal and Plant Health Inspection and Quarantine told the Agence France Presse news agency the virus was discovered from samples sent in by the farm in the southern Pingtung county on March 1. Taiwanese authorities have slaughtered 467,000 birds since H5N2, a less virulent strain of the bird flu which has hit the Asian region, was first detected at a chicken farm in the central county of Canghua on January 15. The origin of the infection remains unknown.

Source: [http://www.abc.net.au/ra/newstories/RANewsStories\\_1062466.htm](http://www.abc.net.au/ra/newstories/RANewsStories_1062466.htm)

14. *March 09, Casper Star-Tribune (Wyoming)* — **More elk die from mystery illness.** Three of four elk captured alive but suffering from a mystery illness that were treated with a regimen of vitamins, antibiotics, and minerals have died or been euthanized, Wyoming Game and Fish Department veterinarian Walt Cook said. **Necropsies on two additional animals have been completed, but analysis of tissues has not been concluded so game officials remain baffled about why more than 290 elk have died, including another nine found in the field by wildlife managers over the weekend. The discovery of the additional nine elk leaves officials disappointed because last week they believed the herd had passed the point where additional animals would become ill.** In all cases the elk seem basically healthy but they lie down and then cannot get back up. In the process to identify the source of malady, Wyoming State Veterinary Laboratory personnel have now ruled out calcium deficiency, chronic wasting disease, bacterial and common viral infections, tick paralysis, and meningeal and carotid artery worm as causes. Mercury poisoning, selenium toxicity, many of the common plant toxins, some insecticides, a variety of metals and salt, nitrate, and sulfate poisoning have also been eliminated.

Source: <http://www.casperstartribune.net/articles/2004/03/09/news/wyoming/89b259efe1cbc51687256e520007af8b.txt>

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

## **Food Sector**

15. *March 09, Interfax* — **Russia bans poultry imports from Maryland. The Russian veterinary authorities on Tuesday, March 9, imposed temporary restrictions on imports**

**of poultry from the state of Maryland.** At the veterinary service, Interfax was told that the ban followed confirmation of a case of bird flu in the state. The restrictions apply to live poultry, incubator eggs, poultry meat, and all types of poultry products not subject to thermal treatment, and also feed and feed additives for poultry. Earlier Russia limited imports from Delaware and Texas because of bird flu. Russia needs an estimated two million tons of poultry a year. The import quota for this year is 1.05 million tons, 771,900 of which is to come from the United States.

Source: [http://www.interfax.ru/e/B/0/26.html?id\\_issue=9678203](http://www.interfax.ru/e/B/0/26.html?id_issue=9678203)

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

## Water Sector

16. *March 08, Water Tech Online* — **EPA water report targets disinfection byproducts. U.S. Environmental Protection Agency (EPA) researchers have quantified the occurrence of more than 200 previously unidentified disinfection by-products (DBPs) for the first time. The EPA has also determined that disinfectants other than chlorine can produce comparable levels of DBPs that may pose health risks.** Using gas chromatography/mass spectrometry (GC/MS), liquid chromatography/mass spectrometry (LC/MS), and gas chromatography/infrared spectroscopy (GC/IR) techniques to identify unknown DBPs, the EPA conducted a nationwide DBP occurrence study of more than 50 unregulated DBPs determined to be of health concern from among some 500 DBPs that have been reported in scientific literature. The EPA team sampled drinking water from a dozen utilities in six regions using water from different sources and quality, including sources with elevated levels of bromide, and disinfecting with chlorine and alternatives such as ozone, chlorine dioxide, and chloramines. Source: [http://www.watertechonline.com/news.asp?mode=4&N\\_ID=46432](http://www.watertechonline.com/news.asp?mode=4&N_ID=46432)

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

## Public Health Sector

17. *March 09, Agricultural Research Service* — **Air curtain blocks insect pests. A system developed by Agricultural Research Service (ARS) scientists uses a curtain of air to prevent disease-carrying insects from boarding airplanes.** Researchers developed a method for using high-velocity air curtains in passenger walkways to provide a barrier against problem insects. Passenger walkways are the bridgelike structures that passengers enter to board the airplane from the gate. **Results of the study show that air curtains can exclude 99 percent of flying insects,** according to Robert K. Vander Meer, acting research leader of the ARS Mosquito and Fly Research Unit. The estimated cost of the two vertically mounted air curtains is about \$3,000. The system provides an alternative to insecticidal methods currently used. The curtain is made of air blown away from the passenger doors by fans on either side of the walkway, at an air speed of at least one meter per second. Insects cannot penetrate the barrier. Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>
18. *March 08, Washington Post* — **Anthrax treatments look promising.** Two experimental drugs designed to treat anthrax infection have shown promise in recent tests, according to their

developers. **A Maryland biotechnology company, plans to reveal March 8 that its anti-anthrax drug appears safe for human use based on a recent test. The company disclosed Sunday, March 7, that separate tests in rabbits suggested the drug might be effective if given within 12 hours of exposure to anthrax.** A second company, located in New Jersey, said a similar anti-anthrax drug it is developing was able, if administered immediately ahead of time, to protect rabbits and mice from the lethal effects of inhaling anthrax spores. The company is not as far along as its Maryland competitor, but so far the two drugs appear quite similar. Most of the test results have not yet been scrutinized by the Food and Drug Administration, and approval, if it comes, could still be several years away. The drugs are artificial antibodies, or proteins that mimic the natural proteins made by the body to fight off invading germs.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A41548-2004Mar 8.html>

**19. *March 08, Associated Press* — Tracking diseases made easier.** Reporting infectious diseases to Illinois officials soon will be a computer-mouse click away. **The Illinois Public Health Department says a Web-based reporting system will help them identify potential bioterrorism and emerging infectious diseases days earlier than the current paper reporting system.** Illinois is installing the electronic reporting system this month at health departments in Chicago and nine counties. **Officials say the system will be running in all 94 local health departments by mid-May and in hospitals and laboratories within five years.** Public Health Director Eric Whitaker says the system will allow the state to track illnesses by address, county, and symptoms. The information can be immediately sent to the U.S. Centers for Disease Control and Prevention.

Source: <http://week.com/morenews/morenews-read.asp?id=3768>

**20. *March 08, Food and Drug Administration* — Guidance issued for developing drugs to treat smallpox vaccine side effects.** The Food and Drug Administration (FDA) Monday, March 8, issued draft guidance for the development of drugs to treat the side effects of vaccination against smallpox with vaccinia virus. **The need for drugs to treat the side effects of the smallpox vaccine became acute after the terrorist attacks on September 11, 2001.** Routine vaccination for smallpox in the U.S. had ended in the 1970s, when the disease stopped occurring naturally, but the potential threat that variola virus would be used as a weapon has raised the possibility that a large-scale vaccination could be necessary in an emergency. **Because the use of this vaccine may cause complications in some individuals, the FDA wants to help commercial and research sponsors plan and design appropriate studies for the development of drugs to treat such adverse events.** The guidance includes sections on chemistry, manufacturing and controls; nonclinical toxicology; microbiology; and clinical pharmacology. The guidance also focuses on the acquisition of in vivo data through the use of animal models. The guidance concludes with sections addressing the acquisition of human efficacy and safety data.

Source: <http://www.fda.gov/bbs/topics/news/2004/NEW01033.html>

[[Return to top](#)]

## **Government Sector**

Nothing to report.

## **Emergency Services Sector**

21. *March 09, Federal Computer Week* — **Governors get secure DHS lines.** By the end of the month, the Department of Homeland Security (DHS) will be able to speak securely with governors' offices in all states and territories, a top department official said this week. **Chief information officer Steve Cooper said the department has links with at least 28 state government offices, and by the end of the month expects to be connected to the rest of the states and territories "so that the secretary or any authorized department official can pick up the phone and have a secure conversation or secure video teleconference with those governmental authorities."** The initiative has been underway for more than a year. Governors initially expressed concerns about getting a secure way to communicate with the federal government in emergencies after the September 11, 2001, terrorist attacks.

Source: <http://fcw.com/geb/articles/2004/0308/web-dhs-03-09-04.asp>

22. *March 09, Reuters* — **Ear print database to finger criminals.** Criminals are used to trying to avoid leaving fingerprints at a crime scene. **But now British scientists have developed a computerized system that allows them to identify ear prints just as easily.** Criminals often wear gloves but are less likely to cover their ears. But before would-be burglars try to pry open a window they might press their ear against the glass to hear if anyone is home. "Basically we have brought it up to speed and modernized things considerably. We've produced a computerized system for identifying ear prints along the lines of the fingerprint system," said Professor Guy Ruttly, head of the forensic pathology unit at the University of Leeds in England. Instead of manually sorting through ear prints and images, Ruttly's system allows investigators to systematically search an ear print database. **Ear prints are taken from about 15 percent of crime scenes in Britain and have already been used to capture culprits in the Netherlands and Switzerland. An ear print can easily be lifted from the window and may help to identify the culprit even if no fingerprints were left behind. Ear prints also leave behind DNA.**

Source: <http://www.cnn.com/2004/TECH/ptech/03/09/science.earprints.reut/index.html>

## **Information and Telecommunications Sector**

23. *March 09, eSecurity Planet* — **Linux privilege escalation hole detected.** According to an advisory from computer security consultants iSEC Security Research, a flaw was found in the Linux kernel memory management code and is completely unrelated to a similar vulnerability reported in February. The flaw carries a "critical" rating and affects Linux versions 2.2 up to and including 2.2.25; it also impacts versions 2.4 up to and including 2.4.24 as well as versions 2.6 up to and including 2.6.2. **"Proper exploitation of this vulnerability leads to local privilege escalation giving an attacker full super-user privileges. The vulnerability may also lead to a denial-of-service attack on the available system memory,"** iSEC warned. Linux distributor Gentoo confirmed its implementation of the open source operating system was susceptible to the flaw and strongly urged users to upgrade to newer, more secure versions.

The flaw was discovered in the memory subsystem which allows for shrinking, growing, and moving of chunks of memory along any of the allocated memory areas which the kernel possesses. iSEC Security Research found that the code doesn't check the return value of the memory function.

Source: <http://www.esecurityplanet.com/trends/article.php/3322911>

24. *March 09, Microsoft* — **Microsoft Security Bulletin MS04–008: Vulnerability in Windows Media Services Could Allow a Denial of Service.** A vulnerability exists because of the way that Windows Media Station Service and Windows Media Monitor Service, components of Windows Media Services, handle TCP/IP connections. **If a remote user were to send a specially–crafted sequence of TCP/IP packets to the listening port of either of these services, the service could stop responding to requests and no additional connections could be made.** The service must be restarted to regain its functionality. Windows Media Unicast Service may also be affected by a successful attack against Windows Media Station Service if Windows Media Unicast Service is sourcing a playlist from Windows Media Station Service. In this case, Windows Media Unicast Service could stop functioning when it encounters the next item in the playlist. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider installing the security update.

Source: <http://www.microsoft.com/technet/security/bulletin/ms04–008.msp>

25. *March 09, Microsoft* — **Microsoft Security Bulletin MS04–009: Vulnerability in Microsoft Outlook Could Allow Code Execution.** A vulnerability in Outlook 2002 caused by the parsing of specially crafted mailto URLs exists could allow Internet Explorer to execute script code in the Local Machine zone on an affected system. To exploit this vulnerability, an attacker would have to host a malicious Website that contained a Web page designed to exploit the vulnerability and then persuade a user to view the Web page. The attacker could also create an HTML e–mail message designed to exploit the vulnerability and persuade the user to view the HTML e–mail message. After the user has visited the malicious Website or viewed the malicious HTML e–mail message an attacker who successfully exploited this vulnerability could access files on a user's system or run arbitrary code on a user's system. **This code would run in the security context of the currently logged–on user.** Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.

Source: <http://www.microsoft.com/technet/security/bulletin/ms04–009.msp>

26. *March 09, Microsoft* — **Microsoft Security Bulletin MS04–010: Vulnerability in MSN Messenger Could Allow Information Disclosure.** A security vulnerability exists in Microsoft MSN Messenger. The vulnerability exists because of the method used by MSN Messenger to handle a file request. An attacker could exploit this vulnerability by sending a specially crafted request to a user running MSN Messenger. **If exploited successfully, the attacker could view the contents of a file on the hard drive without the user's knowledge as long as the attacker knew the location of the file and the user had read access to the file.** To exploit this vulnerability, an attacker would have to know the sign–on name of the MSN Messenger user in order to send the request. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider installing the security update.

Source: <http://www.microsoft.com/technet/security/bulletin/ms04–010.msp>

## Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 1 out of 4 <a href="https://gtoc.iss.net">https://gtoc.iss.net</a>	 Security Focus ThreatCon: 1 out of 4 <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_NETSKY.C</b> Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
<b>Top 10 Target Ports</b>	3127 (mydoom), 135 (epmap), 80 (www), 445 (microsoft-ds), 1434 (ms-sql-m), 137 (netbios-ns), 554 (rtsp), 1080 (socks), 1025 (blackjack), 3128 (squid-http) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center

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

## General Sector

27. *March 09, CNN* — **Zimbabwe on 'alert' over seized jet.** Zimbabwe's government says it has put its army on full alert after seizing a U.S.-registered cargo plane that officials say was carrying 64 suspected mercenaries and a cargo of military gear. **In Washington, a U.S. State Department spokesman said the aircraft had no connection to the U.S. government, and the company listed as the plane's owner said the aircraft was sold recently.** The Boeing 727 was impounded Sunday evening in the capital Harare after authorities concluded its owners had falsely declared the cargo and passengers, who were taken into custody, police spokesperson Wayne Bvudzijena told CNN on Tuesday. "An investigation to establish the true identities of the men and their ultimate mission is under way," he said. "A full statement will be issued in due course." **The jet's owner is listed in U.S. aviation records as Dodson Aviation based in Rantoul, Kansas.** Reached at a Dodson facility in South Africa, company spokesman Jim Pippin said the plane was sold to Logo Logistics in South Africa, although CNN did not immediately find a listing for the company in the national telephone directory.  
 Source: <http://www.cnn.com/2004/WORLD/africa/03/09/zimbabwe.plane/in dex.html>

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

### 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)883-3644

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 703-883-3644 for more information.

### **Contact DHS/IAIP**

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at [nicc@dhs.gov](mailto:nicc@dhs.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.