Department of Homeland Security Daily Open Source Infrastructure Report for 12 October 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a Cessna Citation jet, reported stolen from St. Augustine, was found at the Gwinnett County Airport−Briscoe Field near Atlanta, raising questions of security at the airport, which is the fifth busiest in Georgia and where two September 11 hijackers trained. (See item 11)

- The Associated Press reports flights into Boston's Logan International Airport were delayed again on Tuesday, as federal officials worked for a second day to fix a malfunctioning radar system. (See item 12)

- The Kansas City Star reports Kansas emergency management officials are planning for large−scale evacuations in the event of a catastrophe, and preparing for disasters in other states that might prompt thousands of evacuees to head for Kansas. (See item 21)

- US−CERT has released Technical Cyber Security Alert TA05−284A: Microsoft Windows, Internet Explorer, and Exchange Server vulnerabilities. (See item 23)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact 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://www.esisac.com]

1. *October 11, AFX* — **International Energy Agency says oil market, U.S. economy recovering from hurricanes.** The oil shock from Hurricanes Katrina and Rita hurricanes is blowing itself out but did set back the U.S. economy in the third quarter, the International Energy Agency (IEA) said. U.S. economic growth may have been reduced by a full percentage point in the third quarter but is now showing signs of recovery, the IEA said. The release of oil and oil products from stocks together with market flexibility had absorbed much of the hurricane disruption, the IEA said in its monthly report. However, official bodies might have to take further measures to ward off possible strains in energy markets, it said, in an apparent reference to a possible further release from stockpiles. The IEA estimated that the hurricanes might cut oil production by 77.0 to 104.0 million barrels a day from September to December, and output of liquefied natural gas by 13.0−18.0 million barrels. The IEA reduced its forecast for growth of global oil demand this year by 90,000 barrels a day to 1.26 million barrels a day. In 2006, demand would grow by 1.75 million barrels a day owing to a rebound from "the largely temporary impact of Katrina and Rita and a recovery in Chinese demand."
IEA October Oil Market Report: http://omrpublic.iea.org/
Source: http://www.iii.co.uk/news/?type=afxnews&articleid=5431490&subject=economic&action=article

2. *October 11, Reuters* — **U.S. natural gas supply adequate but expensive this winter, according to association.** There will be enough supplies of U.S. natural gas to meet this winter's demand even with the disruption in offshore gas production caused by the recent hurricanes, but costs will be much higher, the American Gas Association (AGA) said Tuesday, October 11. Helping to ensure there will be plenty of supply is the amount of natural gas stored in underground caverns, which is "on track" to reach 3.2 trillion cubic feet by November 15 at the beginning of the winter heating season, said Paul Wilkinson, AGA vice president for policy analysis. However, between one billion and three billion cubic feet per day of natural gas production in the Gulf of Mexico could still be offline due during the upcoming January−March period due to lingering damage from Hurricanes Rita and Katrina, Wilkinson said. The supply disruption will help push natural costs for consumers "significantly higher" this winter, he said.
AGA Natural Gas Outlook: Winter 2005−2006:
http://www.aga.org/Content/ContentGroups/Public_Relations2/Supply_and_Price/Winter_outlook_consumer_version.pdf
Source: http://www.alertnet.org/thenews/newsdesk/N11468058.htm

3. *October 10, Associated Press* — **Coal deliveries interrupted by heavy rain.** The price of coal mined in Wyoming's Powder River Basin surged to record highs last week, as electric utilities bid aggressively in the market to make up for shipments lost by a host of problems that have dogged coal producers and railroads since May. Most recently, torrential rains in Kansas at the beginning of October washed away hundreds of feet of track on Union Pacific Corp.'s lines near Topeka and damaged several rail bridges. The disruption caused a backup over a hundred trains long, many of them carrying Wyoming coal, and caused several utilities that depend on coal shipped on those lines to run dangerously low on supplies. "It was pretty serious," said Stephen Doyle, a coal market consultant. "It took out a whole week's worth of deliveries from all those lines that feed into Kansas City and St. Louis," said Doyle. Last week's track problems aren't the first of the year. Power plant owners across the Midwest, Great Plains, Southeast and Southwest have been receiving on average about 85 percent of expected coal deliveries since May, after heavy precipitation caused two trains to derail in Wyoming and started a massive

maintenance program by the railroads to repair the track.
Source: http://www.sltrib.com/ci_3104990?rss

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *October 11, Associated Press* — **Biometric ATMs not being used in U.S. because of expense and privacy concerns.** Iris scanning technology has been tested at ATMs in the U.S., but banks haven't embraced the technology because of the expense and the large size of the cameras. The technology is being used internationally, however. In Colombia, South America, biometrics is used in lieu of ATM cards at Ban Café, the fifth−largest bank in the country. Although at the outset the technology proved faulty in some populations, particularly for the worn hands of the elderly and manual laborers, technology improvements have resulted in the rate of undetectable fingerprints falling to two percent from 30 percent. Avivah Litan, an analyst with Gartner Inc., a technology analysis firm, said, "Biometrics is certainly the most secure form of authentication. It's the hardest to imitate and duplicate." Other uses of biometrics include scans to verify the identity of managers at checkout counters who approve customer checks. According to Jim Block, director of Global Advanced Technology at Diebold, "The real holy grail in biometrics is let's get rid of the PIN so no one has anything to steal anymore."
Source: http://www.nytimes.com/aponline/business/AP−Biometric−ATMs.h tml

5. *October 11, Finextra* — **Scottrade to utilize two−factor authentication technology.** Beginning in 2006, the broker will utilize a system that will provide customers with a secret image and phrase that they will look for during their log in on the brokerage site. If customers are able to match their information with that on the site, they will know that the Website is secure and that it is safe to proceed with entering passwords and other information. The system also employs a real−time risk−based decision engine using statistical modeling to authenticate users, assess transactions, and detect fraud.
Source: http://finextra.com/fullstory.asp?id=14376

6. *October 10, Reuters* — **London prepares for large scale financial disaster.** The Bank of England, the British Treasury, and the British Financial Services Authority (FSA)are planning a virtual exercise to test communication and decision making in a mock disaster exercise with 50 firms from the financial services industry, including banks, insurers, and fund managers. Banks participating in the exercise scheduled for November 28 include Credit Suisse First Boston,

Deutsche Bank, and Merrill Lynch. Rob McIvor, spokesperson at the FSA, said "There has always been business continuity planning. We are taking it up a notch this year." Participants will engage in an Internet chatroom designed to help keep financial markets open; the chatroom was initially implemented after the September 11, 2001 attacks, and subsequently implemented in July during the London transport system attacks. Participants will also explore how to keep communications open between institutions during catastrophic events.
Financial Services Authority: http://www.fsa.gov.uk/
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=topNews&storyID=2005−10−10T130113Z_01_KWA046682_RTRUKOC_0_UK−FINANCIAL−FSA−CONTINGENCY.xml&archived=False

7. *October 10, Techweb News* — **Men charged in botnet phished PayPal and eBay accounts.** Three men were arrested in the Netherlands for using the Toxbot, also known as Codbot, Trojan to infect more than 100,000 computers in an attempt to install spyware and adware and to steal PayPal and eBay accounts. Dutch officials said that the attack, which infected computers and servers around the world, is among the largest botnet apprehensions ever. A statement released by the Dutch Public Prosecution Service read, “With 100,000 infected computers, the dismantled botnet is one of the largest ever seen." The hackers subsequently used the hijacked accounts to pay for items they ordered on the Internet. Authorities alleged that they may also have been paid by third parties to create mechanisms to steal the usernames and passwords for online bank accounts. According to Graham Cluley, senior technology consultant for security company Sophos, the Toxbot virus was modified by the hackers many times since its debut in February 2005, which allowed them to keep ahead of anti−virus systems. Cluley added, "This was not just a one−off. The sheer number of variants shows this wasn't a crime they committed just once."
Source: http://www.techweb.com/wire/security/171204478;jsessionid=CIWETEZQUEYXIQSNDBECKHSCJUMEKJVN

8. *October 10, Wall Street Journal* — **Fraud occurs more often through traditional, rather than electronic, means.** According to a joint report released by Javelin Strategy and the Better Business Bureau in January 2005, the most frequently reported source of information used to commit fraud was a lost or stolen wallet or checkbook. The 2005 Javelin Identity Fraud Survey Report revealed that in 2004, computer crimes accounted for 11.6 percent of all known−cause identity fraud (half of the computer crimes resulted from the use of spyware), while 29 percent of victims experienced a lost or stolen wallet, checkbook, or credit card. 2.2 percent of reported fraud was attributed to computer viruses or hackers. The report also found that financial losses attributed to online theft were less than one−eighth the cost of crimes committed via paper statements ($551 average loss through online means versus $4,543 average loss from paper statements). Reports of identity fraud dropped from 10.1 million in 2003 to 9.3 million in 2004. TowerGroup, a division of MasterCard, reports that nearly 50 percent of debit−card fraud occurs through their acquisition by a family member or friend who knows the personal identification number. The Federal Trade Commission reports that identity theft affects almost five percent of adults and costs $53 billion each year.
Source: http://www.post−gazette.com/pg/05283/586015.stm

[Return to top]

Transportation and Border Security Sector

9. *October 11, Business Travel News* — **JetBlue plans major Northeast expansion.** JetBlue Airways on Tuesday, October 11, announced the next wave of new destinations and increased frequencies from Boston and New York JFK, including 10 daily flights between the two cities. The airline said it would deploy the first of its new 100−seat Embraer 190 aircraft to handle service expansion. Boston−New York JFK flights will start November 19 and ramp up by December 20. By offering such frequent service in the busy Northeast Corridor, JetBlue will battle for frequent travelers against Delta's and US Airways' shuttle operations at LaGuardia, multiple daily flights offered by American at all three major New York metropolitan−area airports, a deep Continental schedule at Newark and intercity Amtrak rail service. Meanwhile, JetBlue in Boston in the coming months plans to add service to four new destinations, in addition to New York JFK. They include Austin; Nassau, Bahamas; Richmond and West Palm Beach.
Source: http://www.btnmag.com/businesstravelnews/headlines/article_display.jsp?vnu_content_id=1001263927

10. *October 11, Associated Press* — **Police: Man takes over train with bow and arrow.** In a confrontation reminiscent of the Wild West, police shot and wounded a man who allegedly took over a freight train with a bow and arrow. Juventino Vallejo−Camerena boarded the Union Pacific train Sunday night, October 9, as it was stopped for a signal in western San Bernardino County, CA, and threatened the engineer and conductor, the only people on board, police Capt. Keith Jones said. The crew members escaped and disabled the train by turning off fuel switches, then used a cell phone to call police, Union Pacific spokesperson Mark Davis said. "The employees did an outstanding job," Davis said. "Their instincts took over and they did the proper thing by disabling the train." Vallejo−Camerena was treated at a hospital, then booked into jail for investigation of train robbery, assault and resisting arrest. The locomotive, en route to Los Angeles from Salt Lake City, was hauling 71 cars with ocean−bound containers. No hazardous materials were on board, Davis said.
Source: http://www.boston.com/news/nation/articles/2005/10/11/police_man_takes_train_with_bow_and_arrow/

11. *October 11, Associated Press* — **Jet stolen from Florida winds up near Atlanta.** A 10−passenger Cessna Citation jet, reported stolen from St. Augustine, FL, was found at the Gwinnett County Airport−Briscoe Field early Monday, October 10, said Darren Moloney, spokesperson for the Gwinnett County Police Department. The FBI is also investigating although the theft does not appear to be linked to terrorism, said Lisa Ray, spokesperson at the Georgia Office of Homeland Security. It had some damage to the front edge of one wing but was not disabled, authorities said. Although the plane landed when the airport's flight tower was not operating, officials said that is not unusual. The Federal Aviation Administration (FAA) is probing its own traffic system to see if there is any record of the plane flying during the time in question, FAA spokesperson Kathleen Bergen said. Planes are easy to steal if you know how to fly them, because they usually do not require a key to start the engines, Gwinnett County Police Sgt. D. Mattox said. Ray had no comment on whether this latest incident raised larger questions of security at the airport, which is the fifth busiest in Georgia. Two of the September 11 hijackers, trained there for a time.
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−s

tolen−airplane,0,6048273.story?coll=sns−ap−nation−headlines

12. *October 11, Associated Press* — **Radar problem delays Boston flights again.** Flights into Boston's Logan International Airport were delayed again Tuesday, October 11, as federal officials worked for a second day to fix a malfunctioning radar system. The radar systems were showing "false targets" −− blips that air traffic controllers knew were not planes in flight, said Federal Aviation Administration (FAA) spokesperson Arlene Murray. Incoming flights were delayed over two hours on average Tuesday, an airport spokesperson said. Logan's radar surveillance system first broke down on Monday, when many flights were more than four hours late arriving. A New Jersey−based FAA team was in Boston to investigate the problem, Murray said. Flights were being monitored by a long−range backup radar system in Nashua, NH, Murray said. Relying on that system requires increasing the distance between planes from three miles to five miles, resulting in the delays.
    Source: http://www.usatoday.com/travel/news/2005−10−10−logan−delays_x.htm

[Return to top]

Postal and Shipping Sector

13. *October 11, Transport Topics* — **Velocity Express, Greyhound set new delivery service.** Velocity Express Corp. and Greyhound PackageXpress, the package−delivery unit of Greyhound Lines, announced Monday, October 10, they have signed an agreement to provide package−delivery services between key metropolitan areas. To be called Metro−to−Metro Guaranteed Package Delivery Today, the initiative will leverage Greyhound Lines' round−the−clock schedule of intercity departures and available cargo space on each bus with Velocity's door−to−door pick up and delivery capabilities, Velocity said in a statement. One delivery service will guarantee door−to−door pick up and delivery within 10 hours, while one will guarantee overnight service with delivery as early as 6:30 a.m. The services begin immediately with the following city pairs: New York and Boston, New York and Philadelphia, and Dallas and Houston. Additional city pairs will be added in the coming months, Velocity said.
    Source: http://www.ttnews.com/members/topnews/0014021.html

[Return to top]

Agriculture Sector

14. *October 11, The Ledger (FL)* — **Citrus greening cases double.** The number of confirmed cases of the fatal citrus greening disease in Florida has doubled in the past 10 days and may have reached as far north as Palm Beach County, the third Southeast Florida county to show signs of infection. State inspectors have confirmed citrus greening on 161 trees on 140 properties across Miami−Dade and Broward counties, said Denise Feiber, an agriculture department spokesperson. Inspectors also have found suspected cases in several Palm Beach communities, including Delray Beach, Boca Raton and West Palm Beach, she added. Greening is a bacterial disease first discovered in southern Dade in late August. It eventually kills the tree, but before that the plant produces misshapen fruit with a bitter flavor unsuitable for the

juice or fresh markets. The farther the disease spreads, the more unlikely state agriculture officials can prevent a statewide outbreak, according to Timothy Gottwald, a plant pathologist with the U.S. Department of Agriculture lab in Fort Pierce.
Information on citrus greening disease:
http://www.aphis.usda.gov/ppq/ep/citrus_greening/index.html
Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20051011/NEWS/510110328/1001/RSS02&source=RSS

15. *October 11, TheNewMexicoChannel.com* — **Veterinarians warn of pigeon fever.** Veterinarians are warning horse owners in the Bloomfield, NM, area to be on the lookout for a disease known as pigeon fever. Four horses have been affected and veterinarians say they're not exactly sure how it's being spread. Dr. Charles Lange has treated three of the four horses in Bloomfield to come down with the pigeon fever. He said the disease can cause internal abscesses that can kill an animal if left untreated. The disease is rarely fatal. Lange said while he's not exactly sure how it's being carried, it could be in the Bloomfield irrigation system, which is commonly used for animals' water supply. Lange said pigeon fever is can also be spread by biting fleas that get into boils and carry the bacteria to other animals.
Source: http://www.thenewmexicochannel.com/news/5082246/detail.html

[Return to top]

Food Sector

Nothing to report.

[Return to top]

Water Sector

16. *October 11, Rochester Democrat and Chronicle (NY)* — **Legionnaires' disease found in Brighton.** A resident at The Friendly Home nursing home in Brighton, NY, has tested positive for Legionnaires' disease, an illness that made recent news after a devastating outbreak at a Toronto, Canada nursing home. Legionnaires' disease, a type of pneumonia, is contracted after directly inhaling mist or vapor contaminated with Legionella bacteria −− mist that typically emanates from a shower, hot tub or large air conditioning system. Bill Kouwe, chief operating officer of The Friendly Home, said the resident is the only case of Legionnaires' that has surfaced there. The nursing home learned the resident had the illness October 3. Representatives from the New York state Health Department tested water from the nursing home's hot water tanks, showerheads and faucets Friday, October 7, for signs of the bacteria. Kouwe said the testing did not involve the air conditioning system, as it does not have a water tank associated with it. Kouwe said The Friendly Home now occasionally will raise the temperature of its hot water tanks to kill any existing bacteria and will do routine testing of water throughout the facility.
Source: http://www.democratandchronicle.com/apps/pbcs.dll/article?AID=/20051011/NEWS01/510110333/1002/NEWS

[Return to top]

Public Health Sector

17. *October 11, Mirror (United Kingdom)* — **Tests for bird flu negative in Romania.** Fears that a deadly bird flu strain had spread to Romania may be wrong. Experts believed H5N1, the strain behind 65 deaths in Asia, had entered Europe for the first time after three ducks died. But initial tests for avian flu viruses were "negative," the Department for Environment, Food and Rural Affairs said. Debby Reynolds, chief veterinary officer of the United Kingdom, added that a European Union team would fly to Romania Tuesday, October 11, to carry out more tests. She also confirmed a bird flu strain may have been found in Turkey, and added the United Kingdom and European Union were ready to take "swift action to reduce any chance of the disease spreading." Defra said no samples had yet been sent to Britain from Romania for testing.
Source: http://www.mirror.co.uk/news/tm_objectid=16229024&method=full&siteid=94762&headline=tests−for−bird−flu−−negative−−in−rom ania−−name_page.html

18. *October 11, Media Line* — **Middle East prepares for bird flu.** Middle Eastern countries are preparing for an outbreak of avian influenza. Jordan has established a national committee to combat the danger of the disease spreading, after several cases of the disease were detected last week in Turkey. Jordan took measures following predictions from health experts that the disease might affect the region. Israel’s Health Ministry published a report on Sunday, October 9, detailing instructions for workers in the poultry farming industry on how to protect themselves against bird flu. Other Middle Eastern countries are planning a meeting in Egypt at the end of November to coordinate ways to prevent the disease from spreading. According to the London−based A−Sharq Al−Awsat, the meeting will take place Monday, November 28, in cooperation with the World Health Organization.
Source: http://themedialine.org/news/news_detail.asp?NewsID=11507

19. *October 11, Bloomberg* — **Indonesia's fifth human bird flu case is confirmed.** The World Health Organization (WHO) confirmed Indonesia's fifth human case of avian influenza after a 21−year−old man in the Lampung province in Sumatra tested positive for the virus. An "initial investigation has revealed that the man had direct exposure to diseased and dying chickens in his household shortly before the onset of illness," according to a statement on the United Nations Website. Three of the five confirmed cases in Indonesia were fatal, the WHO said. Avian flu cases may increase in Indonesia as the wet season, which typically begins in November and runs until April, starts, said the WHO on Monday, October 3. There are 98 people across the nation currently under observation for bird flu, I Nyoman Kandun, director general of disease control and environmental sanitation at the Health Ministry, said in a phone interview Tuesday, October 11. The cases are spread over nine of Indonesia's 33 provinces, he said. U.S. Health and Human Services Secretary Michael Leavitt, who is visiting Thailand, Vietnam, Laos and Cambodia this week to discuss bird flu, Monday, October 10, urged countries to increase their capacities to manufacture antiviral drugs and vaccines.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=aNuPNHNmdUxY&refer=asia

20. *October 11, Cheboygan Daily Tribune (MI)* — **Cheboygan Memorial Hospital's bioterrorism exercise is largest ever in Northern Michigan.** Cheboygan Memorial Hospital (CMH) officials and staff in Cheboygan, MI, participated in an emergency preparedness drill

Tuesday, October 11, in hopes of improving communication in the event of a disaster. The bioterrorism exercise is the largest ever held in Northern Michigan, said Nancy Gagnon, manager of emergency services for CMH. Gagnon stated that two key objectives of the drill included revising CMH's public information policies as well as improving their communication. She said the drill was not limited to CMH and included all of "Region 7," which spans eight or nine counties from south of Traverse City to Mackinaw City in Michigan. A total of 17 counties were actually involved in the drill. The event was spearheaded by the Region 7 Healthcare Disaster Preparedness Project. The group has been working with health care and other critical partners to help prepare Northern Michigan for emergencies such as acts of terrorism, natural disasters, industrial accidents, mass−casualty incidents and many other tragic events, said Tres Brooke, bioterrorism preparedness coordinator for Region 7. The drill is funded by a $1.3 million grant through the state and the National Hospital Bioterrorism Preparedness Program.
Source: http://www.cheboygannews.com/articles/2005/10/11/news/news4. txt

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

21. *October 11, Kansas City Star* — **Kansas revises disaster plans.** Kansas emergency management officials aren't satisfied planning just for the state's trifecta of disasters: floods, tornadoes and ice storms. Hence, they've also drawn up plans for earthquakes, bioterrorism, plague, livestock disease, nuclear attack, a nuclear reactor meltdown and toxic spills. Now, in the aftermath of Hurricane Katrina, they're preparing for disasters in other states that might prompt thousands of evacuees to head for Kansas. Because of the response to Hurricane Katrina, Kansas Governor Kathleen Sebelius has asked Emergency Management Division officials to take another look at all its plans. Preparation for ice storms, tornadoes and flooding occupies most of the state's disaster−planning energies. But an entire section of the Emergency Management Division is dedicated to planning for large−scale evacuations in the event of a wider catastrophe.
Source: http://www.kansascity.com/mld/kansascity/news/local/12869716 .htm

22. *October 10, Watertown Daily Times (WI)* — **Wisconsin to host full−scale exercise with National Guard.** Wisconsin Governor Jim Doyle said Friday, October 7, state officials are not prepared to handle mass evacuations if a large disaster or catastrophe were to take place in the state. Watertown, WI, officials will get a chance to prove the governor wrong during a full−scale Wisconsin National Guard exercise in the city on Saturday, October 15. The full−scale exercise, which involves 300 Guard members, will begin at noon Saturday and will continue into Sunday morning. In conjunction with the National Guard exercise, Watertown officials will conduct a functional exercise of their Emergency Operation Center on Saturday from 10 a.m. to 2 p.m. CDT. Watertown officials could be confronted with such simulated situations as tornadoes, animal disease outbreaks, explosives, manmade disasters or cracked

pipelines. The purpose of these exercises is to find out what the gaps might be during responses and to be able to correct them. The exercises are scheduled to be conducted in the vicinity of the Watertown Municipal Building, Watertown Airport, Calvary Baptist Church and the National Guard Armory. The purpose of the National Guard exercise is to familiarize local officials in a multiagency response to a terrorism event.
Source: http://www.wdtimes.com/articles/2005/10/10/news/news3.txt

[Return to top]

Information Technology and Telecommunications Sector

23. *October 11, US−CERT* — **Technical Cyber Security Alert TA05−284A: Microsoft Windows, Internet Explorer, and Exchange Server vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Windows, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on an affected system. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges or with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take complete control of an affected system. An attacker may also be able to cause a denial of service.
Updates are available on the Microsoft Update site:
http://www.microsoft.com/technet/security/bulletin/ms05−oct. mspx
Source: http://www.us−cert.gov/cas/alerts/SA05−284A.html

24. *October 10, Security Focus* — **Kaspersky Anti−Virus Engine CHM file parser remote buffer overflow vulnerability.** Kaspersky Anti−Virus Engine is prone to a remote buffer overflow vulnerability. This issue presents itself when an attacker sends a maliciously crafted CHM file to an affected computer and this file is processed by Kaspersky's CHM file parser. This vulnerability allows attackers to execute arbitrary machine code in the context of the affected application. Attackers may gain privileged remote access to computers running the affected application. The vendor has released a signature update to address this issue. Users with updated signatures released after July 2005 are not vulnerable.
Source: http://www.securityfocus.com/bid/15054/info

25. *October 10, FrSIRT* — **Computer Associates iGateway remote buffer overflow vulnerability.** A vulnerability has been identified in various Computer Associates products, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error in the iGateway component that does not properly handle specially crafted HTTP GET requests (port 5250) when debug mode is enabled, which could be exploited by remote attackers to execute arbitrary commands and compromise a vulnerable system. No solution is currently available.
Source: http://www.frsirt.com/english/advisories/2005/2028

26. *October 10, Security Focus* — **PHPMyAdmin local file include vulnerability.** phpMyAdmin is prone to a local file include vulnerability. An attacker may leverage this issue to execute arbitrary server−side script code that resides on an affected computer with the privileges of the

Web server process. This may potentially facilitate unauthorized access. phpMyAdmin 2.6.4−pl1 is reported to be vulnerable. Other versions may be affected as well. There are no vendor−supplied patches currently available for this issue.
Source: http://www.securityfocus.com/bid/15053/info

27. *October 10, SecuriTeam* — **Shorewall MACLIST security vulnerability.** The Shoreline Firewall, "more commonly known as 'Shorewall', is a high−level tool for configuring Netfilter. You describe your firewall/gateway requirements using entries in a set of configuration files". A problem has been reported in the Shorewall Firewall that enables a Client accepted by MAC−Filter to bypass any other rule. This Issue doesn't apply to any Shorewall Version before 2.2.0. Users of any version before 2.2.5 are encouraged to update to a newer version (at least 2.2.5, better 2.4.1) of Shorewall. Shorewall Version 2.0.x is still supported, but Users of 2.0.x are encouraged to upgrade to a newer version.
Source: http://www.securiteam.com/unixfocus/6F00C00EAM.html

28. *October 10, FrSIRT* — **imapproxy "ParseBannerAndCapability" format string vulnerability.** A vulnerability has been identified in imapproxy, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a format string error in the "ParseBannerAndCapability()" [main.c] function that does not properly handle a specially crafted banner/capability line received from the server, which could be exploited by remote attackers to compromise a vulnerable system by convincing a user to connect to a specially crafted IMAP server. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/2014

29. *October 10, FrSIRT* — **Utopia News Pro SQL injection and cross−site scripting vulnerabilities.** Two vulnerabilities were identified in Utopia News Pro, which could be exploited by malicious users to perform SQL injection or cross site scripting attacks. The first issue is due to an input validation in the "header.php" and "footer.php" scripts when processing a specially crafted "sitetitle" or "version" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. The second vulnerability is due to an input validation error in "news.php" when processing a specially crafted "newsid" parameter, which may be exploited by remote users to conduct SQL injection attacks. Utopia News Pro version 1.1.4 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/2012

30. *October 10, Security Focus* — **Linux Kernel multiple security vulnerabilities.** Linux kernel is prone to multiple vulnerabilities. These issues may allow local and remote attackers to trigger denial of service conditions or disclose sensitive kernel memory. Linux kernel 2.6.x versions are known to be vulnerable at the moment. Other versions may be affected as well.
Various patches are available to address these issues:
http://www.securityfocus.com/bid/15049/references
Source: http://www.securityfocus.com/bid/15049/references

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a format string vulnerability in the Helix Player. Please note that this vulnerability affects all media players based on the Helix Player, such as Real Player on UNIX / LINUX systems. The vulnerability exists in the way Helix Player handles certain media files. A remote attacker who is able to convince a user to view a specially crafted media file, may be able to execute arbitrary code with the privileges of the Helix Player process.

More information about this vulnerability can be found in the following US−CERT Vulnerability Note:
* VU#361181 − Helix Player format string vulnerability

Until a patch is available to address this vulnerability, US−CERT strongly encourages users to review the workarounds section of the Vulnerability Note (VU#361181).

Top Source Port / IP Addresses: Increased reported port activity: 1028 UDP, 1029 UDP, 1030 UDP, 1434 UPD from the following IP blocks, located in China: 222.77.185.242, 220.164.140.140, 221.10.254.31, 218.27.16.180, 222.77.185.228, 222.241.95.6 , 218.66.104.186, and 220.164.141.140

US−CERT warns users to expect an increase in targeted phishing emails due to recent events such as Hurricane Katrina and Hurricane Rita. For more information please refer to: http://www.us−cert.gov/current/#kat

US−CERT strongly recommends that all users reference the Federal Emergency Management Agency (FEMA) Website for a list of legitimate charities to donate to their charity of choice. http://www.fema.gov/

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 6881 (bittorrent), 1026 (win−rpc), 5498 (hotline), 445 (microsoft−ds), 40000 (−−−), 135 (epmap), 139 (netbios−ssn), 25 (smtp), 5328 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure 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 ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.