Department of Homeland Security Daily Open Source Infrastructure Report for 29 July 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

Please Help Improve the DHS Daily Infrastructure Report

We are striving to improve the DHS Daily Infrastructure Report for all of our readers. Please help us in this effort by filling out a short feedback form, which can be found by clicking on this link:

http://chrome.osis.gov/questionnaire

The form will only be available for two weeks, so please fill it out at your earliest convenience. Thank you in advance.

Daily Highlights

- The Department of Homeland Security will install radio frequency technology at five border posts with Canada and Mexico to track foreigners driving in and out of the United States. (See item 6)
- Government Technology reports Long Beach Airport is implementing a sophisticated wireless video surveillance platform that will enable security operations centers to simultaneously monitor distant sites. (See item 7)
- The USDA said Wednesday that testing of a 12−year−old cow yielded possible signs of bovine spongiform encephalopathy, and that further tests are being conducted to clarify whether the disease was present. (See item 15)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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. *July 28, RenewableEnergyAccess.com* — **Illinois enacts requirement for renewable energy.** Following more than five months of public comment and deliberation, the Illinois Commerce Commission (ICC) adopted Governor Blagojevich's Sustainable Energy Plan. Under the ICC's plan, a new Renewable Portfolio Standard, or RPS, will require the state's electric utilities to draw on renewable energy sources for two percent of their electricity needs by the end of 2006. After that, the requirement will increase by one percent per year until 2012, when it tops out at eight percent. In addition to renewables, there's also a component for energy efficiency. Under the Energy Efficiency Portfolio Standard utility companies will create new programs to reduce 10 percent of rising electricity demand by 2007 by helping their customers invest in energy saving equipment and technology. By 2015, these energy efficiency programs will reduce 25 percent of Illinois' increasing energy demand. The ICC expects Illinois' electric utilities to file plans to implement the Sustainable Energy Plan within 30 days. This move brings to 19 the number of states, including the District of Columbia, that have legislated a state−wide requirement for renewable energy.
   Source: http://www.renewableenergyaccess.com/rea/news/story;jsessionid=a3dr2FmExew9?id=34813

2. *July 28, Washington Post* — **Storms knock out power to over 100,000.** Swift thunderstorms pounded the Washington, DC, area on Wednesday, July 27, leaving more than 150,000 homes without electricity. Utilities officials said that some customers could be without power until Friday, July 29. "We're saying 8 p.m. Friday for [restoration of power to] the very last customer," said Pepco utility spokesperson Mary−Beth Hutchinson. The storms were triggered by a cold front entering the region from the west that clashed with the hot, humid air mass that had stalled over the region in recent days, said Calvin Meadows, a meteorological technician for the National Weather Service in Sterling. Temperatures reportedly plummeted about 20 degrees in three hours, bringing readings in the low−70s for the first time in several days.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/27/AR2005072700446.html?nav=rss_metro/dc

3. *July 28, Australian Associated Press* — **Bomb threat shuts refinery in Australia.** A man is being questioned after a bomb threat was made against Queensland, Australia's largest petroleum fuels refinery. About 700 workers were evacuated by police at 10:30am (AEST) on Thursday, July 28, when an anonymous caller threatened to blow up the Caltex Australia site. A thorough search by a police bomb squad failed to find any traces of explosives. A police spokesperson confirmed that a man had been taken in for questioning over the threat. The refinery, the fifth largest in Australia, was commissioned in 1965 and has a crude oil throughput of 4.4 million gallons per day.
   Source: http://www.smh.com.au/news/National/Bomb−threat−shuts−refinery−in−Brisbane/2005/07/28/1122143947333.html?oneclick=true

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *July 27, Government Accountability Office* — **GAO−05−687: Defense Ammunition: DoD Meeting Small and Medium Caliber Ammunition Needs, but Additional Actions Are Necessary (Report).** Following the end of the Cold War, the Department of Defense (DoD) significantly reduced its purchases of small and medium caliber ammunition and reduced the number of government−owned plants that produce small and medium caliber ammunition. Since 2000, however, DoD's requirements for these types of ammunition have increased notably. Because the success of military operations depends in part on DoD having a sufficient national technology and industrial base to meet its ammunition needs, the Government Accountability Office (GAO) was asked to review DoD's ability to assess if its supplier base can meet small and medium caliber ammunition needs. Specifically, GAO (1) identified changes over the past several years that have increased the requirement for small and medium caliber ammunition, (2) assessed the actions DoD has taken to address the increased requirement, and (3) determined how DoD plans to ensure that it can meet future small and medium caliber ammunition needs. GAO is making recommendations aimed at strengthening DoD's ability to implement its plan and ensure accountability. In commenting on a draft of this report, DoD concurred with GAO's recommendations and provided information on its planned steps to implement them.
   Highlights: http://www.gao.gov/highlights/d05687high.pdf
   Source: http://www.gao.gov/new.items/d05687.pdf

[Return to top]

Banking and Finance Sector

5. *July 29, The Epoch Times (NY)* — **Phishing attacks dampen Internet business.** A recent Gartner survey of 5,000 online buyers found that phishing has increased by nearly 30 percent during 2005. Gartner, an international information technology industry provider, suggests that consumer confidence concerning online purchases and financial activities may drop substantially, resulting in a one to three percent decrease in online business. Gartner analysts said most online consumers do not open e−mail from companies or individuals they do not know from prior experience. Three of every four online shoppers said they are more cautious about where they buy goods online, and one of three report buying fewer items than they otherwise would because of security concerns. More than 80 percent of U.S. online consumers said their concerns about online attacks have affected their trust in e−mail from companies or individuals they don't know personally. Of these consumers, more than 85 percent delete suspect e−mail without opening it. "This figure has serious implications for banks and other

companies that want to use the e−mail channel to communicate more cost−effectively with their customer base," said Avivah Litan, vice president and research director at Gartner.
Gartner survey: http://www.gartner.com/press_releases/asset_129754_11.html
Source: http://www.theepochtimes.com/news/5−7−28/30694.html

[Return to top]

Transportation and Border Security Sector

6. *July 28, Associated Press* — **DHS to launch radio frequency systems at border crossings.** The Department of Homeland Security (DHS) will install radio frequency technology at five border posts with Canada and Mexico to track foreigners driving in and out of the United States. In its ongoing efforts to tighten border security and monitor possible terrorist and criminal activity, Bob Mocny of DHS said the wireless chips for vehicles would become mandatory at designated border crossings in Canada and Mexico as of next Thursday, August 4. After a foreigner entering the U.S. has passed a thorough security check once, they will be given a document containing the chip. This document will need to be renewed every six months. The document must be placed on the dashboard of a car so that a person's personal information can be read as they approach a border crossing. Even with the radio frequency technology, however, the vehicle will still have to stop. If a person's identifying data produce no red flags, they will get just a cursory check at the border rather than lengthy questioning. The mandatory program will apply, however, to all foreigners with U.S. visas −− including those from the 27 countries whose citizens don't need visas for short U.S. visits −− who cross into the United States at those points.
Information about US−VISIT: http://www.dhs.gov/dhspublic/display?theme=91
Source: http://informationweek.com/story/showArticle.jhtml?articleID =166403260

7. *July 28, Government Technology* — **California airport implements wireless video surveillance system.** Long Beach Airport in southern Los Angeles County, has selected BroadWare Technologies, Inc. to implement a sophisticated wireless video surveillance platform. The airport, an alternate to Los Angeles International Airport, hosts major airlines such as Alaska Airlines, American Airlines, America West Airlines and JetBlue Airways. The new wireless surveillance system will enable three separate Long Beach Airport security operations centers to simultaneously monitor distant sites, including secured airport areas, public parking lots and roadway tunnels. This system provides a single wireless solution for viewing, storing and managing real−time video from more than 100 cameras, becomes one of the very first wireless surveillance systems to be installed at any airport in the U.S. This cost−effective, easy−to−use, integrated security platform provides Long Beach Airport with the necessary technology to respond more effectively and recover more rapidly from security threats and events. With the infrastructure, personnel at three locations in Long Beach (the Command and Control Center, the Security Operations Center and the Security and Safety Office) will be able to monitor information while viewing live video feeds at the same time from the same PC.
Source: http://govtech.net/news/news.php?id=95712

8. *July 27, Transportation Security Administration* — **Sioux Falls Regional Airport to join Screening Partnership Program.** The Transportation Security Administration (TSA)

announced on Wednesday, July 27, approval of Sioux Falls Regional Airport in South Dakota for participation in the Screening Partnership Program (SPP). TSA also announced that 34 companies have been approved as Qualified Vendors, eligible to compete to provide passenger and baggage screening services for the airports that are approved for the SPP. Starting this fall, the Sioux Falls airport will begin the transition from federal TSA security screeners to using screeners employed by a qualified private company. Under the SPP, the federal security director is still responsible for security at the airport and for maintaining TSA security standards. Under a pilot program required by the Aviation and Transportation Security Act, TSA selected airports in five cities to have screeners employed by qualified private companies: San Francisco; Kansas City, MO; Rochester, NY; Tupelo, MS; and Jackson, WY. Private screening companies may only hire employees who meet the same requirements as federal screeners. To date, seven airports −− Sioux Falls Regional Airport, Elko (NV) Regional Airport, and the original five pilot airports −− have applied to the SPP. In addition to Sioux Falls, the original five pilot airports have also been approved and will continue to have private screeners.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 0150f8b

[Return to top]

Postal and Shipping Sector

9. *July 27, WMTW (ME)* — **U.S Postal Service unveils system to detect anthrax in Maine.** Staff at the U.S. Postal Service (USPS) processing center in Portland, ME, unveiled their new biohazard detection system (BDS) on Wednesday, July 27. BDS is a high−tech system that can detect the presence of anthrax in pieces of mail. Whenever mail is sorted, the BDS is activated. Air samples are then taken, and DNA tests are run to check for anthrax and other hazardous materials. Portland's BDS became operational last week.
Source: http://www.wmtw.com/news/4776153/detail.html?rss=port&psp=ne ws

[Return to top]

Agriculture Sector

10. *July 28, Kentucky Ag Connection* — **Kentucky expands vesicular stomatitis embargo.** The Kentucky Department of Agriculture (KDA) has expanded its vesicular stomatitis (VS) embargo to 20 counties in Arizona, Colorado, New Mexico, and Utah. Four counties were added to Kentucky's embargo on Tuesday, July 26, after the U.S. Department of Agriculture confirmed cases in La Plata and Mesa counties in Colorado, Rio Arriba County in New Mexico and Grand County in Utah. All livestock, wild and exotic animals from the 20 counties are prohibited from entering Kentucky. Animals from areas of the four affected states not covered by the embargo are required to meet certain conditions before they may enter the Commonwealth. VS is a viral disease that occurs sporadically in the U.S., usually in southwestern states. It can affect horses, cattle and swine, and occasionally sheep, goats and deer. It causes blisters to form in the animal's mouth, on teats or along the hooves, resulting in excessive salivation, lameness or oozing sores. It is not fully known how VS is spread, but insects, mechanical transmission and movement of animals are all factors. Once VS is

introduced into a herd, the disease may move from animal to animal by contact or exposure to saliva or fluid from ruptured lesions.
Source: http://www.kentuckyagconnection.com/story−state.cfm?Id=411&y r=2005

11. *July 28, Xinhuanet (China)* — **Beijing to build animal disease prevention center.** Beijing, China, will spend nearly $12.5 million to build an animal disease prevention and control center, said an official with the municipal veterinary station Thursday, July 28. The center will include a command center, a check−up and diagnosis center, a center to test animal product safety, a service building, and other facilities. The center will collect, analyze and deal with information concerning various animal diseases, diagnose outbreaks of diseases, and test veterinary medicines. Liu Yaqing, deputy director of the municipal agriculture bureau, said that Beijing will reinforce prevention and control work of five animal related diseases, as well as monitoring of animal farms, slaughterhouses, and other related sites.
Source: http://news.xinhuanet.com/english/2005−07/28/content_3279893 .htm

12. *July 28, Grand forks Herald (ND)* — **More cases of anthrax reported in North Dakota.** State officials say North Dakota could see a record number of anthrax cases in livestock this year. Ten more cases were confirmed Wednesday, July 27, in southeastern North Dakota. More than 100 animals have died from the disease since it was first detected July 6 in a bison herd and a cattle herd in Ransom County, State Veterinarian Susan Keller said. Heavy rain has created prime conditions for the spread of anthrax, she said. Spores from bacteria that cause the disease can lay dormant in the soil for decades, but flooding can release the spores to the ground's surface, where livestock graze and become infected, Keller said. The anthrax outbreak has killed livestock on 48 farms and ranches in Barnes, Dickey, LaMoure, Ransom, and Sargent counties this year.
Source: http://www.grandforks.com/mld/grandforks/news/12245310.htm

13. *July 27, U.S. Department of Agriculture* — **USDA designates counties in Illinois as agricultural disaster areas.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Thursday, July 27, designated counties in Illinois as primary agricultural disaster areas. The 93 following counties were designated as primary disaster areas due to drought. Eight additional counties are, also, eligible because they are contiguous. Alexander County is the only county in the state that will not be eligible for emergency loans as a result of this declaration.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?conten tidonly=true&contentid=2005/07/0281.xml

14. *July 26, StopSoybeanRust* — **Soybean rust found in Georgia.** Asian soybean rust was confirmed Wednesday, July 26, on two leaves out of a 100−leaf sample at the Georgia sentinel plots at the Sunbelt Expo in Colquitt, GA. The county is directly southwest of Tift County, where rust was found in a sentinel plot on July 18. The Sunbelt Agricultural Exposition is held at Moultrie, GA, which is the Colquitt county seat in the center of the county. This year's Sunbelt Expo, an annual event, is set for October 18−20, 2005. This find brings the 2005 infected Georgia county count to four: Colquitt, Decatur, Seminole, and Tift. There are now 14 U.S. counties overall found to have rust this year −− either on soybeans, volunteer soybeans, or on kudzu.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=482

[Return to top]

Food Sector

15. *July 28, CIDRAP News* — **USDA to run more tests in possible bovine spongiform encephalopathy case.** Federal officials said Wednesday, July 27, that testing of a 12−year−old cow yielded possible signs of bovine sponiform encephalopathy (BSE), and that further tests are being conducted to clarify whether the disease was present. The carcass was destroyed and did not enter the human food or animal feed chain, said John Clifford, chief veterinarian for the U.S. Department of Agriculture (USDA). The cow died of calving complications on a farm in April. A private veterinarian took a sample of brain tissue but forgot to send it to the USDA for testing until last week. Clifford said the veterinarian preserved the sample in formalin, which is suitable for the immunohistochemistry (IHC) test for BSE but rules out the use of rapid screening tests and the Western blot test. Use of the preservative was permitted under USDA guidelines at the time, but the protocols were changed in June to require that samples be sent in while still fresh. Calling the original IHC test on the sample "nondefinitive," Clifford said it revealed some staining indicating the abnormal prion protein associated with BSE, but it "did not match a normal pattern" for BSE. He said the USDA decided to run additional IHC tests at its national laboratory, and also send samples to the BSE reference lab in England.
Statement by Chief Veterinary Medical Officer John Clifford, Animal and Plant Health Inspection Service: http://www.aphis.usda.gov/lpa/news/2005/07/bsestatement_vs.h tml
Source: http://www.cidrap.umn.edu/cidrap/content/other/bse/news/july 2805bse.html

[Return to top]

Water Sector

16. *July 28, Standard Times (RI)* — **Despite chlorination, Rhode Island city must boil water.** Just days after a steady dose of chlorine was added to many of the town's water wells, fecal coliform bacteria has again been found. Now, for the fourth time in five years, a boil−water advisory has been issued to most North Kingstown, RI, residents. Residents in the Slocum and Saunderstown areas, as well as the Rhode Island Port Authority have been exempted from the advisory. The town began chlorinating the water last Wednesday, July 20, after numerous tests throughout the month of June showed the presence of coliform. However, follow−up tests revealed there to be no sign of fecal coliform, which is a bacteria caused by animal or human waste and could cause diarrhea, nausea and headaches. The bacteria could be especially dangerous for infants, the elderly and those with compromised immune systems. According to a memorandum from the town, the North Kingstown Department of Water Supply anticipates that the wells will be rid of the bacteria "once an adequate chlorine residual is established in the distribution system." At Monday night's town council meeting, Town Manager Richard Kerbel said residents were informed of the advisory Sunday, July 24, via an area−wide recorded message. However, he added that there were some residents who didn't receive a call.
Source: http://www.zwire.com/site/news.cfm?newsid=14937092&BRD=1715&PAG=461&dept_id=73974&rfi=6

[Return to top]

Public Health Sector

17. *July 28, Reuters* — **China bacteria outbreak worsens.** The number of people infected by what Chinese authorities believe is a pig−borne bacterial disease has risen by 14 to 131, state media said on Thursday, July 28. The World Health Organization (WHO) said it was watching developments closely, but a spokesperson said the disease appeared to be localized. China's Ministry of Health said another three people had died from the infection, bringing the death toll to 27. Streptococcus suis, known as swine flu, is endemic in swine in most pig−rearing countries in the world but human infections are rare. Swine flu is not known to have ever been passed between humans, but scientists fear it could mutate into a strain that could easily pass among people. Compounded with its deadliness, such a bug could unleash an epidemic, killing many people. The unusually high mortality rate and reports that many of the victims died within 24 hours of showing symptoms have led some experts to wonder if it is indeed swine flu at all. "It could be another disease altogther, it need not be streptococcus suis because the presentation is so atypical," said Samson Wong, a microbiology associate professor at the University of Hong Kong.
Source: http://www.alertnet.org/thenews/newsdesk/PEK9397.htm

18. *July 28, Daily News Transcript (MA)* — **Walpole develops outbreak response plan.** Walpole, MA, has completed a plan for coordinating health and medical services during an infectious disease outbreak. The plan −− developed over six months with assistance from the state Department of Public Health (DPH) −− outlines how the town would administer drugs and vaccines within three days of an outbreak. Such outbreaks would include smallpox, influenza, Hepatitis A, and meningitis. The plan states that in a declared emergency, the DPH −− working through the state Emergency Management Agency −− will distribute vaccines and medical supplies to two emergency dispensing sites. Both locations will have an coordinator to oversee operations. A team of nurses will also be stationed at three secondary sites. In the event of an emergency, the town, would use what is known as an Incident Command Structure (ICS), a procedure used to coordinate resources and personnel who respond to emergencies. According to the plan, ICS is built around five major components: command, logistics, planning, finance and operations.
Source: http://www.dailynewstranscript.com/localRegional/view.bg?art icleid=60659

19. *July 26, United Press International* — **Bird flu poses risk to vaccine egg supply.** Some infectious disease experts fear an outbreak of bird flu could destroy the supply of chicken eggs needed to produce the annual supply of flu vaccine. The deadly strain of bird flu currently in Asia could spread to the U.S. or be introduced into poultry flocks here intentionally by terrorists, said Greg Poland, an infectious diseases expert at Mayo Clinic in Rochester, MN. He said all U.S. infected flocks would have to be destroyed −− more than 100 million birds in Asia have been destroyed or killed by the flu virus. Bruce Gellin, director of the National Vaccine Program, said health officials have taken precautions to protect chicken flocks that produce eggs for manufacturing vaccines. "These flocks are well−protected," Gellin told UPI. In addition to keeping the chickens isolated from other flocks and wild birds, there is limited access to the farms where they reside, Gellin said, adding that the farms are subject to regular inspections to ensure all of the required biosecurity provisions are in place. There are, also, more chickens than need, so in the event a flock does become infected, there would be surplus

fowl available to meet egg−production needs.
Source: http://www.sciencedaily.com/upi/index.php?feed=Science&article=UPI−1−20050726−12390000−bc−us−birdflu.xml

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

20. *July 28, Medford Transcript (MA)* — **First responders perform a water rescue drill.** Last week officials from the Medford Police Department, Fire Department, Park Police, Recreation Department and Armstrong EMS personnel descended on Wright's Pond in Medford, MA, to perform a water rescue drill, using a lifelike dummy to demonstrate life−saving techniques. One of the first practices was the rescuing a "swimmer" who was injured, but conscious. The majority of the staff stabilized a dummy in the water while another informed recreational officers who, in turn, called in Fire Department and EMS personnel. The drill also focused on controlling bystanders, gathering information on the victim and clearing the beach area so that rescue crews could perform their jobs. A second drill consisted of rescuing a "swimmer" who was face down, unconscious and had apparently suffered cardiac arrest. Again a dummy was stabilized in the water by lifeguards while the proper authorities were notified. The drill differed from the first as lifeguards administered CPR to the victim. Firefighters also practiced an additional one drill, retrieving an "unconscious" dummy in an inflatable raft. After each drill all agencies involved exchanged feedback and gave some initial assessments of the quality of drill and its participants.
Source: http://www2.townonline.com/medford/localRegional/view.bg?articleid=293385

[Return to top]

Information Technology and Telecommunications Sector

21. *July 27, FrSIRT* — **Cisco IOS unspecified remote heap overflow vulnerability.** A vulnerability was identified in Cisco Internet Operating System (IOS), which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a heap overflow error when processing specially crafted packets, which could be exploited by an unauthenticated attacker to execute arbitrary code and compromise a vulnerable device. Cisco IOS version 12.x and 11.x l are affected. It is reported that the vendor has addressed this vulnerability in an April firmware release.
Source: http://www.frsirt.com/english/advisories/2005/1248

22. *July 27, FrSIRT* — **Sophos AntiVirus products remote heap overflow vulnerability.** A critical vulnerability was identified in multiple Sophos AntiVirus products, which may be exploited by remote attackers or malware to execute arbitrary code. This flaw is due to a heap

overflow error when analyzing malformed files, which may be exploited by an unauthenticated remote attacker to execute arbitrary commands by sending an e−mail containing a specially crafted attachment to a vulnerable system. No further details have been disclosed. The following products are affected: Sophos Anti−Virus versions prior to 3.96.0 (on Windows, Unix, NetWare, OS/2, OpenVMS); Sophos Anti−Virus versions prior to 4.5.4 (on all platforms); and Sophos Anti−Virus Small Business Edition Sophos Anti−Virus Small Business Edition will be updated by July 29.
Users should upgrade to Sophos Anti−Virus version 3.96.0 or 4.5.4:
http://www.sophos.com/support/updates
Source: http://www.frsirt.com/english/advisories/2005/1244

23. *July 27, FrSIRT* — **Ethereal Multiple Protocol Dissector and Zlib vulnerabilities.** Multiple vulnerabilities were identified in Ethereal, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. The first issue is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. Various buffer overflow, format string, and null pointer vulnerabilities were identified in the LDAP, AgentX, 802.3, PER, DHCP, BER, MEGACO, GIOP, SMB, WBXML, H1, DOCSIS, SMPP, HTTP, DCERPC, CAMEL, RADIUS, Telnet, IS−IS LSP and NCP dissectors, which could be exploited by attackers to compromise a vulnerable system or cause the application to crash. Ethereal versions 0.8.5 through 0.10.11 are affected.
Users should upgrade to Ethereal version 0.10.12: http://www.ethereal.com/download.html
Source: http://www.frsirt.com/english/advisories/2005/1237

24. *July 27, Security Focus* — **Novell GroupWise Client remote buffer overflow vulnerability.** Novell GroupWise Client is affected by a remote buffer overflow vulnerability. Specifically, this vulnerability arises when a user attempts to log in to a GroupWise post office that contains a malicious 'GWVW02??.INI' file. This can facilitate unauthorized access in the context of the user. This issue affects all versions of Novell GroupWise 6.5 client dated prior to July 15, 2005. Novell has released Technical Information Documents TID10098314 and TID2971927 including GroupWise 6.5 SP5 Client rev 6 to address this issue.
Source: http://www.securityfocus.com/bid/14398/discuss

25. *July 27, FrSIRT* — **VBZooM "SubjectID" parameter remote SQL injection vulnerability.** A vulnerability was identified in VBZooM, which may be exploited by remote attackers to execute arbitrary SQL commands. This flaw is due to an input validation error in the "show.php" script when processing a specially crafted "SubjectID" parameter, which may be exploited by remote users to conduct SQL injection attacks. VBZooM version 1.11 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/1234

26. *July 27, zone−h* — **IPSec Incorrect key usage in AES−XCBC−MAC.** IPsec is a security protocol for the Internet Protocol networking layer. It provides a combination of encryption and authentication of system, using several possible cryptography algorithms. A programming error in the implementation of the AES−XCBC−MAC algorithm for authentication resulted in a constant key being used instead of the key specified by the system administrator. If the

AES−XCBC−MAC algorithm is used for authentication in the absence of any encryption, then an attacker may be able to forge packets which appear to originate from a different system and thereby succeed in establishing an IPsec session. If access to sensitive information or systems is controlled based on the identity of the source system, this may result in information disclosure or privilege escalation.
Source: http://www.zone−h.org/advisories/read/id=7851

27. *July 27, Security Focus* — **Mozilla Suite And Firefox multiple script manager security bypass vulnerabilities.** Multiple issues exist in Mozilla Suite and Firefox. These issues allow attackers to bypass security checks in the script security manager. Security checks in the script security manager are designed to prevent script injection vulnerabilities. An attacker sending certain undisclosed JavaScript in 'view−source:', and 'jar:' pseudo protocol URIs, may bypass these security checks. These vulnerabilities allow remote attackers to execute script code with elevated privileges, leading to the installation and execution of malicious applications on an affected computer. Cross−site scripting, and other attacks are also likely possible. The vendor has released an advisory, as well as upgraded versions of Mozilla Suite, and Mozilla Firefox to resolve these issues.
Source: http://www.securityfocus.com/bid/13641/info

28. *July 27, FrSIRT* — **eMule Kad Packets remote Denial of Service and Zlib vulnerabilities.** Multiple vulnerabilities were identified in eMule, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. The first issue is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. The second vulnerability is due to an unspecified error when processing malformed Kad packets, which could be exploited by remote attackers to cause a denial of service. eMule version 0.46b and prior are affected. Users should upgrade to eMule version 0.46c
Source: http://www.frsirt.com/english/advisories/2005/1238

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 reports a Cisco IOS vulnerability that may allow an unauthenticated, remote attacker to execute arbitrary code. US−CERT generally recommends that organizations that are using Cisco products upgrade to the current updated versions of IOS. According to Cisco, if you have upgraded your Cisco IOS firmware since April 2005, it negates the proof−of−concept exploit code that targeted a previously undisclosed attack vector affecting the Cisco IOS. US−CERT was assured that the code is NOT publicly available. However, users can expect such code targeting this attack vector being

openly developed. Cisco has been made aware of the vulnerability and is working with US−CERT. All readers are encouraged to ensure that their respective enterprises are utilizing IOS firmware dated April 2005 or later. If you are utilizing IOS firmware dated earlier then April 2005 US−CERT suggest that you upgrade to the latest Cisco IOS firmware. Please visit www.cisco.com/security or contact Cisco directly through your support channels. IMPACT: Successful exploitation may result in the execution of arbitrary code that allows an attacker to enter “enable” mode or crash the router. RECOMMENDATIONS: Please update your Cisco IOS to insure you are protected against this new exploit. SYSTEMS AFFECTED: All Cisco IOS versions prior to April, 2005.

Current Port Attacks

Top 10 Target Ports	1026 (−−−), 445 (microsoft−ds), 27015 (halflife), 1433 (ms−sql−s), 6881 (bittorrent), 139 (netbios−ssn), 135 (epmap), 53 (domain), 25 (smtp), 113 (auth) 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

29. *July 27, Gazette (CO)* — **Colorado school officers convene.** More than 125 police officers arrived in Colorado Springs, CO, on Tuesday, July 26, to attend school safety classes, such as bomb threat management, gang updates, and Internet safety, at the 9th Annual Colorado Association of School Resource Officers Conference. The conference runs through Friday, July 29, and provides the latest information and trends, and a chance for officers to network about what’s going on in their schools. Speaking at the conference, Colorado Attorney General John Suthers passed on recommendations from the Columbine Review Commission stressing that schools must have an emergency crisis plan and a threat assessment team. Officers also had a chance to learn about hot spots where problems occur on or near school grounds, how to prevent suicides among students, and how to identify a credible threat and act quickly. Source: http://www.gazette.com/display.php?id=1309326&secid=1

[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