



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 31 March 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- TheOmahaChannel reports a security breach at an Omaha Public Power District substation, where two 13,800–volt power lines were cut, has the power provider reviewing its security policies. (See item [1](#))
- Reuters reports more than 700 additional Border Patrol agents will be sent to Arizona to help stop potential terrorists and illegal immigrants from entering the United States from Mexico, increasing the total number of border agents in Arizona to about 3,000. (See item [11](#))
- The Union Leader reports New Hampshire has become the first state to install a secure satellite communications system to connect more than 600 law enforcement agencies, fire departments, emergency medical services, and hospitals with the Department of Homeland Security. (See item [22](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [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 Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & 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://esisac.com>]

1. *March 29, TheOmahaChannel (NE)* — **Power line intentionally cut.** A security breach at an Omaha Public Power District (OPPD) substation has the power provider reviewing its security policies. Someone broke into OPPD's property at 4th and Marcy streets and cut two 13,800–volt power lines. Omaha police believe the person who cut the lines is seriously

burned. When OPPD employees got to the scene, they found a saw and smelled burned flesh. The break in happened Sunday, March 27, at about 11:30 a.m. One power line was completely cut. It's a back-up circuit for part of downtown Omaha's power. Another line was damaged. OPPD believes the person who cut the lines may be homeless. There are several homeless people who frequent the area of the substation. OPPD also thinks the person may have been trying to steal the lines for the copper that's inside.

Source: <http://www.theomahachannel.com/news/4328111/detail.html?rss=oma&psp=news>

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

Chemical Industry and Hazardous Materials Sector

2. *March 30, Associated Press* — **Chlorine spill in China responsible for deaths and mass evacuation.** A truck loaded with 33 tons of chlorine overturned near the city of Hui'an in Jiangsu province in eastern China on Tuesday, March 29, spewing fumes that killed 27 people and left another 285 hospitalized, Chinese government officials said Wednesday. More than 10,000 people were evacuated after the accident.
Source: <http://www.baltimoresun.com/news/nationworld/world/wire/sns-ap-china-chlorine-leak.1.628151.story?coll=sns-ap-world-headlines>
3. *March 30, WTVO (IL)* — **Hazmat crew called after accident at pork plant.** Hazmat crews were summoned to a chemical emergency, and two employees at the Pork King Packing plant in Merengo, IL, were taken to Woodstock Memorial Hospital after being overwhelmed by chlorine-like fumes, according to Marengo Fire Battalion Chief Jeff Kimmel. It took over three hours for the Hazmat team to clean up, after monitoring air quality, trying to stop the leak and keeping the spill contained. Pork King Packing President Tom Miles says the hazardous materials were created in a chemical reaction during a routine delivery of cleaning supplies. The operator of the delivery truck poured the wrong chemicals inside the plant, causing a violent gaseous reaction.
Source: <http://www.wtvo.com/Global/story.asp?S=3141474&nav=7kXRY3RH>
4. *March 30, WKYC (OH)* — **Ohio interstate shut down after chemical spill.** Akron, OH, firefighters say a tractor-trailer carrying animal-based acid flipped on Interstate-76 westbound at State Route 224, on Wednesday, March 30. Police shut east and west bound traffic on I-76, which has been diverted to State Route 224, until further notice. The Environmental Protection agency was called to the scene. However, officials said the chemical spill is a minimal hazard to the environment. The truck was carrying eight barrels of oleoylscrocinic acid, which is used in pharmaceutical and cosmetic products.
Source: http://www.wkyc.com/news/news_fullstory.asp?id=32561
5. *March 29, Auburn Journal (CA)* — **California officials close section of interstate after toxic spill.** A hazardous substance spill closed parts of Interstate 80 in Truckee, CA, just west of Reno, NV, for more than four hours Tuesday, March 29, beginning at about 9:00 a.m. The driver of a Federal Express semi-truck noticed a toxic smell and a dripping liquid coming from his truck and radioed California Highway Patrol (CHP) to investigate. The substance the driver was transporting was heptane, a flammable gas used for camp stove cooking. Mark Dinger, a

public information officer for the California Department of Transportation (Caltrans), said the fuel was being transported in five 328-gallon totes. One leaked about half of its contents, spilling approximately 164 gallons.

Source: http://www.auburnjournal.com/articles/2005/03/30/news/top_stories/01spill.txt

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

Defense Industrial Base Sector

Nothing to report.

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

Banking and Finance Sector

6. *March 30, Reuters* — **Officials with Japan's Mizuho Bank say customer data lost.** Officials with Japan's Mizuho Bank said on Wednesday, March 30, that confidential account data on 270,000 customers has been lost. The retail banking arm of Japan's biggest lender, Mizuho Financial Group, said data including customers' names, account numbers and transaction histories had been lost at 167 branches over a span of several years. The bank said an internal investigation had uncovered no evidence that the data had been leaked to outsiders or misused. "There is a high probability that the information was accidentally disposed of, and it is extremely unlikely that it was passed to outside parties," the bank said in a statement. Mizuho has approximately 30 million account holders, the most of any Japanese bank.
Source: <http://news.ft.com/cms/s/594c85b0-a0da-11d9-95e5-00000e2511c8.html>

7. *March 30, Canadian Press* — **Canadians fear identity theft over virus attacks.** Thirty-nine per cent of Canadians consider identity theft, such as having passwords and personal information stolen, to be their primary security concern online, according to a recent study. However, 64 percent of Canadians surveyed were unable to accurately define the term phishing. In rating security, men and women differed slightly in their online priorities in the study. Forty-two percent of women versus 36 percent of men rated identity theft as their number one concern. However, more men (22 percent) than women (10 percent) rated spyware or adware tracking their online habits as their primary online security concern. Study: <http://www.aol.ca/portal/about/press.adp>
Source: <http://www.canada.com/businesscentre/story.html?id=fd104ea0-837f-484f-9a6d-8d191ee0d740>

8. *March 29, IDG News Service* — **Personal data protection tightened in Japan.** Beginning Friday, April 1, businesses throughout Japan, including foreign companies, must comply with legislation that sets out new rules for handling personal data. The Personal Information Protection Law applies to any company with offices in Japan that holds personal data on 5,000 or more individuals, according to Kazuhito Masui, an attorney at Shiba International Law Offices, a major international law firm based in Tokyo. Personal data as defined by the law includes a person's name, address, date of birth, sex, home and mobile phone numbers, and also a person's e-mail address if that address is recognizably the person's name. The law and guidelines represent a significant step forward in making personal data more secure in Japan,

experts said. "It's an attempt to make companies more responsible," said Kazuo Makino, a professor of law at Kokushikan University. While the penalties set for noncompliance to the law are low, the legislation should prove effective in making companies tighten their security because of the damaging publicity that might arise if they are found guilty, Makino said.

Source: <http://www.pcworld.com/news/article/0,aid,120219,00.asp>

9. *February 28, Government Accountability Office* — **GAO-05-199: Catastrophe Risk: U.S. and European Approaches to Insure Natural Catastrophe and Terrorism Risks (Report)**. Natural catastrophes and terrorist attacks can place enormous financial demands on the insurance industry, result in sharply higher premiums and substantially reduced coverage. As a result, interest has been raised in mechanisms to increase the capacity of the insurance industry to manage these types of events. The Government Accountability Office (GAO) in this report (1) provides an overview of the insurance industry's current capacity to cover natural catastrophic risk and discusses the impacts of the 2004 hurricanes; (2) analyzes the potential of catastrophe bonds — a type of security issued by insurers and reinsurers (companies that offer insurance to insurance companies) and sold to institutional investors — and tax deductible reserves to enhance private-sector capacity; and (3) describes the approaches that six European countries have taken to address natural and terrorist catastrophe risk, including whether these countries permit insurers to use tax-deductible reserves for such events. We provided a draft of this report to the Department of the Treasury and the National Association of Insurance Commissioners. Treasury provided technical comments that were incorporated as appropriate. Highlights: <http://www.gao.gov/highlights/d05199high.pdf>
Source: <http://www.gao.gov/new.items/d05199.pdf>

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

Transportation Sector

10. *March 30, Associated Press* — **Number of civil aviation accidents down in 2004**. The number of civil aviation accidents in the United States fell by eight percent last year, according to preliminary statistics released Tuesday, March 29. The National Transportation Safety Board (NTSB) reported that civil aviation accidents declined from 1,864 in 2003 to 1,715 last year. There were also nine percent fewer deaths in 2004 — 635, down from 695 the year before. Most aviation fatalities resulted from accidents involving private planes and on-demand air taxis, but the overall accident rate for both kinds of aircraft has been improving over the past few decades. There were 68 accidents involving air taxis, or charter planes, last year, seven fewer than the 75 reported the year before. The number of people who died in air taxi accidents rose 55 percent last year, to 65, from 42 the previous year. Paul Czysz, professor emeritus of aviation and engineering at St. Louis University, said one reason for the improving safety record of charter planes is that more experienced pilots are now flying them.
Source: <http://www.cnn.com/2005/TRAVEL/03/30/aviation.accidents.ap/>
11. *March 30, Reuters* — **DHS officials to increase security on border with Mexico**. More than 700 additional Border Patrol agents will be sent to Arizona this year to help stop potential terrorists and illegal immigrants from entering the United States from Mexico, officials said on Wednesday, March 30. Department of Homeland Security officials said an additional 534 agents would be permanently assigned to the border and 200 others would be sent on temporary

duty for fiscal year 2005 to crack down on illegal immigration and disrupt smuggling operations. The changes would boost the total number of border agents in Arizona to about 3,000, officials said. Last year about 1.2 million illegal immigrants were caught crossing the 2,000-mile U.S.–Mexico border and about 40 percent of them in the deserts of Arizona. Nearly 385,000 were caught in Arizona between March and September 2004, during the first phase of the Arizona Border Control Initiative, according to Homeland Security figures. Officials said the boost in resources has also led to jumps in narcotics seizures and decreased the number of border crossing–related deaths.

Source: <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=8033201>

12. *March 30, Reuters* — Airline officials resist proposal on safety reporting. Officials with big airlines and other aviation companies are resisting some or all of a proposal to broaden requirements for reporting safety incidents to federal transportation investigators. The National Transportation Safety Board proposed a regulation in December 2004 to ensure that accident investigators are notified promptly and fully when several types of incidents occur involving jetliners, private planes, and helicopters. Investigators want to tighten accident–reporting rules with commercial and business jet operations, which are growing at a record pace. But airlines like United Airlines, aerospace manufacturers like Boeing, helicopter makers, and leading pilot groups object to some or all of the changes. The Air Transport Association, the leading trade group for U.S. airlines, said direct reporting of engine failures and anti–collision alerts "is neither necessary nor beneficial." The association said, "Collection and reporting of this data beyond existing Federal Aviation Administration reporting requirements would be resource–intensive, duplicative, and non–productive."

Source: http://www.usatoday.com/travel/news/2005-03-30-airlines-ntsb_x.htm

13. *March 30, Anchorage Daily News (AK)* — Automatic ID system is a step toward safer shipping. The Coast Guard will begin tracking ship traffic electronically through the Aleutian Islands this summer, providing data that eventually could demonstrate the need for new equipment to prevent shipwrecks in the heavily traveled region, agency officials said Tuesday, March 29, at a shipping safety forum in Anchorage. While the Coast Guard has little authority over "vessels of innocent passage," new federal security laws require all ships to transmit information about themselves when passing through U.S. waters. Shore–based receivers pick up the information, including the name and size of the vessel, its course and its speed. The technology is already being used elsewhere in Alaska, including Southeast and Cook Inlet, said Capt. Jack Davin, the Coast Guard's chief of marine safety in Alaska. The next receiver will be set up on the edge of 25–mile–wide Unimak Pass. Over time, the Coast Guard will develop solid information rather than estimates on vessel traffic in the region. Other ideas about improving shipping safety and oil spill response in the North Pacific were discussed at Tuesday's forum, which was organized by the University of Alaska Marine Advisory Program and the Alaska Oceans Program. University of Alaska Marine Advisory Program:

<http://www.uaf.edu/map/>. Alaska Oceans Program: <http://www.alaskaoceans.net/index.htm>

Source: <http://www.adn.com/news/alaska/story/6325227p-6201910c.html>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

14. *March 29, Agence France Presse* — British vets sound alarm as hospital bacteria spreads to animals. The antibiotic-resistant bacteria methicillin-resistant Staphylococcus aureus (MRSA), which has killed hundreds of people in Britain, is now spreading among pets and farm animals, the head of a veterinary group warned. "There have been cases of MRSA in the veterinary population and these are of great concern to veterinary surgeons here and abroad," said Bob Partridge, president of the British Veterinary Hospitals Association. "The main concern is trying to ensure we have as few cases as possible by encouraging veterinary surgeons to adopt best practice in operating procedures," he said. Partridge noted that the present level of animal infection was relatively low, with just 10 to 20 cases reported in Britain annually for the past two to three years.

Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=11&u=/afp/20050329/hl_afp/healthsuperbugbritain_0503291_83422

15. *March 29, Associated Press* — Terrorism bill would stiffen penalties for animal rights threats. A terrorism bill would add Ohio to a growing number of states seeking harsher penalties for attacks by animal rights activists and environmentalists, including those against dog food makers, farms where animals are caged, and university animal labs. Arson, vandalism, assault, break-ins, and other tactics used by extremists already are illegal. A 1992 federal law forbids interfering with "an animal enterprise" but enforcement is difficult, said FBI Special Agent James Turgal, who heads the agency's Ohio terrorism unit. He said the state ecoterrorism bills could allow more federal terrorism prosecutions under the Patriot Act. Only a small percentage of the FBI's active terrorism investigations in Ohio involve environmental activists, but they are increasing, he said. States have taken varied approaches. A proposed bill in New York would ban any attempt to impede animal research or commerce, forbid financial donations to "animal or ecological terrorist organizations" and create a registry of such groups. Pennsylvania's bill, like Ohio's, creates harsher penalties for people convicted of vandalism, assault, or other offenses if they involve intimidation or obstruction of legal research and commerce involving animals and natural resources.

Source: <http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--eco-terrorism0329mar29.0.3640433.story?coll=ny-region-apnewyork>

16. *March 28, Brookhaven National Laboratory* — Use of functional imaging to track plant nutrients has many potential applications. Scientists at the U.S. Department of Energy's Brookhaven National Laboratory have applied some of the same techniques used in medical imaging to track the distribution of nutrients in poplar trees in response to a simulated insect attack. The research provides new insights on a long-debated theory about how plants respond to environmental stress, and shows that radio-tracer imaging can be a big help in unraveling plant biochemistry. "This enables us to study the effects of external factors like insect attacks, disease, elevated carbon dioxide, soil toxins, and drought on vital plant processes," said Richard Ferrieri, who leads Brookhaven's role in the research. To simulate an insect attack, the scientists painted a solution of jasmonic acid, a chemical messenger that plants produce in response to various types of stress, onto the leaves of poplar trees in a closed chamber. They

then administered carbon dioxide gas labeled with radioactive carbon-11 to individual leaves, where it is quickly converted to sugar, and traced the movement of this radio-labeled sugar through the plants using autoradiography and other techniques. Autoradiography allows for taking a snapshot in time showing the precise location of the radio-tracer within the plant.

Source: http://www.bnl.gov/bnlweb/pubaf/pr/PR_display.asp?prID=05-30

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

Food Sector

Nothing to report.

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

Water Sector

17. *March 30, Government Accountability Office* — GAO-05-283: Klamath River Basin: Reclamation Met Its Water Bank Obligations, but Information Provided to Water Bank Stakeholders Could Be Improved (Report). Drought conditions along the Oregon and California border since 2000 have made it difficult for the Bureau of Reclamation (Reclamation) to meet Klamath Project irrigation demands and Klamath River flow requirements for threatened salmon. To augment river flows and avoid jeopardizing the salmon's existence, Reclamation established a multiyear water bank as part of its Klamath Project operations for 2002 through 2011. Water banks facilitate the transfer of water entitlements between users. This report addresses (1) how Reclamation operated the water bank and its cost from 2002 through 2004, (2) whether Reclamation met its annual water bank obligations each year, (3) the water bank's impact on water availability and use in the Klamath River Basin, and (4) alternative approaches for achieving the water bank's objectives. Government Accountability Office (GAO) recommends that Reclamation improve the information provided to stakeholders by systematically providing public information on management decisions and the water bank's status. The Departments of Commerce and the Interior reviewed a draft of this report and generally agreed with the findings; Reclamation agreed with the recommendation. Highlights: <http://www.gao.gov/highlights/d05283high.pdf>
Source: <http://www.gao.gov/new.items/d05283.pdf>

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

Public Health Sector

18. *March 30, Agence France Presse* — Health alerts issued in African countries as Angola struggles with Marburg epidemic. At least three African nations are on alert after an outbreak of Marburg virus claimed a record toll in Angola. Health alerts have been issued in the Democratic Republic of Congo, which borders Angola and where the second highest number of deaths due to the virus was previously recorded, in Congo-Brazzaville and as far as the eastern African country of Kenya. Kenya's health ministry said Wednesday, March 30, it had set up a system at the country's two main airports in Nairobi and Mombasa to screen passengers arriving from Angola. An alert was issued to all hospitals and clinics in Kenya, which recorded three

cases of the disease in the 1980s. Angola's neighbor, the Democratic Republic of Congo (DRC) went on high alert Tuesday, March 29, issuing protective kits. Congo has also stepped up health controls along its border with DRC in order to reduce the possibility of the outbreak spreading, the health ministry said.

Source: <http://www.reliefweb.int/rw/RWB.NSF/db900SID/EVIU-6AYF6P?OpenDocument>

19. *March 30, United Press International* — Petting zoo kidney disease numbers rise in Florida.

The number of kidney infections that may be linked to petting zoos has risen to 17 and possibly 20 with reports of new cases on Florida's west coast. Fourteen children and three adults have been confirmed with a strain of E. coli after attending either the Florida Strawberry Festival in Plant City, FL, or the Central Florida Fair in Orlando. Orange County, where the Central Florida Fair is held, had the most cases. Among the new confirmed and unconfirmed cases were five in the Tampa Bay area and one just to the north of there. All of the patients tested positive for the specific type of E. coli, or showed symptoms of having hemolytic uremic syndrome, a complication of the infection that can be deadly. One 12-year-old girl has died and officials were waiting for the results of tests to determine the exact cause.

Source: http://washingtontimes.com/upi-breaking/20050330-095139-3949_r.htm

20. *March 30, New York Times* — Tests pending in cases tied to drug-resistant HIV strain.

Investigators looking into the possible spread of a virulent strain of HIV detected in a New York City man have identified several patients who may have a related strain of the virus, but the investigators have cautioned that they cannot yet say if the cases are connected, officials with the city's Department of Health and Mental Hygiene said Tuesday, March 29. Because of the complexity of the lab testing involved in matching strains of the virus, it could be months before health officials will be able to determine if others have indeed been infected with the dangerous strain. Health officials said that his case was particularly troubling because it was the first in which they had seen a strain of the virus that was both resistant to nearly all drug treatments and highly aggressive, leading rapidly from HIV infection to AIDS.

Source: <http://www.nytimes.com/2005/03/30/nyregion/30aids.html>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

21. *March 30, The Arizona Republic* — Arizona officials meet to discuss communications, security issues.

More than three years after the 9/11 attack, Arizona's terrorism response system remains stymied by a communications clog: firefighters, police officers and other emergency workers sometimes cannot talk to each other because their radio systems aren't synchronized. This and other issues were discussed at a statewide Homeland Security Summit on Tuesday, March 29, drew more than 200 Arizona civil defense leaders to Phoenix.

Authorities say the solution involves a lot of money to buy new communications gear. But

spending alone won't help, because there is no way to require agencies to purchase uniform equipment. Faced with diminishing federal funding, officials have established advisory councils in the state so that anti-terrorism equipment and programs are shared by communities in five regions: north, east, south, west and central. Members of the councils met privately Tuesday to discuss terrorism vulnerabilities -- what they need to prevent attacks, and how they can best respond when catastrophe strikes. Besides solving the radio communications problem, they said, Arizona needs its border with Mexico secured, formal emergency-response pacts with Indian tribes and shared terrorism intelligence.

Source: http://www.azcentral.com/arizonarepublic/local/articles/0330_homeland30.html

22. *March 30, The Union Leader (NH)* — **New Hampshire officials unveil new communications system.** New Hampshire has become the first state in the nation to install a secure satellite communications system to connect more than 600 law enforcement agencies, fire departments, emergency medical services and hospitals with the U.S. Department of Homeland Security (DHS). Called the Homeland One First Responder Network, the new system links fire, police and emergency services into one network that provides communications between those agencies and enables fire and police personnel to access up-to-date training modules to keep up with new training requirements and developments. Homeland One's training programs include the Law Enforcement Training Network, and the Health & Sciences Network. It is partnered with Homeland One Net, which provides online tests for first responders to take after viewing Homeland One training programs, allowing them to manage compliance training, gain certification and track progress. The law enforcement curriculum covers topics such as profiling terrorist groups, crime scene investigation, tactical patrol and weapons of mass destruction, said Director of Police Standards & Training Keith Loman.

Source: http://www.theunionleader.com/articles_showfast.html?article=52630

23. *March 30, Daily News Tribune (MA)* — **Massachusetts cities get communications vans for emergencies.** Waltham, Pittsfield, Holyoke, Worcester, Taunton and Lowell were chosen to host \$267,000, state-of-the-art Field Communication Vehicles. The vehicles include several mobile radios, video links to the state police air wing, onboard weather stations, GPS systems, wireless computers and hydraulic light towers. They were purchased with \$1.6 million in federal fiscal 2003 Department of Homeland Security grants awarded by the Executive Office of Public Safety to the Fire Chiefs Association of Massachusetts.

Source: <http://www.dailynewstribune.com/localRegional/view.bg?articleid=53170>

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

Information Technology and Telecommunications Sector

24. *March 30, Secunia* — **MIT Kerberos telnet client has buffer overflow vulnerabilities.** Two vulnerabilities have been reported in Kerberos V5, which can be exploited by malicious people to compromise a vulnerable system. A boundary error in the "slc_add_reply()" function in the included telnet client when handling LINEMODE sub-options can be exploited to cause buffer overflow via a specially crafted reply containing a large number of SLC (Set Local Character) commands. A boundary error in the "env_opt_add()" function in the included telnet client when handling NEW-ENVIRON sub-options can be exploited to cause a heap-based buffer overflow via a specially crafted reply containing a large number of characters that need

escaping. Original advisory and patch available at:

<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2005-001-telnet.txt>

Source: <http://secunia.com/advisories/14745/>

25. *March 29, SecurityTracker* — **phpCOIN lets remote users inject SQL commands and execute arbitrary files on the target system.** A vulnerability was reported in phpCOIN. A remote user can execute arbitrary files located on the target system. A remote user can also inject SQL commands. The software does not properly validate user-supplied input in the search engine query, the username and email fields when requesting a forgotten password, and in the domain name field when ordering a product. A remote user can supply specially crafted values to execute SQL commands on the underlying database. The vendor has issued a fixed version (1.2.2), available at: <http://www.phpcoin.com/auxpage.php?page=download>
Source: <http://securitytracker.com/alerts/2005/Mar/1013592.html>

26. *March 28, Symantec* — **Multiple Symantec products have denial of service vulnerabilities.** Two vulnerabilities were reported in Symantec's Norton AntiVirus, Internet Security, and System Works in the AutoProtect feature. A user can create a file or modify a filename to cause the target system to crash. When AutoProtect was invoked to scan a particular file type, e.g., introduced on a CD, copied and pasted into the system, etc., the resultant scan caused the system to hang and generate a general protection fault error, or BSOD requiring a system reboot to clear. When SmartScan enabled, renaming a file stored on a network share can induce a system crash when the modification kicks off SmartScan. Based on the file write for the name change, SmartScan will be invoked to scan the file, which can result in excess CPU consumption and ultimately a system crash. Updates are available via Symantec LiveUpdate.
Source: <http://securityresponse.symantec.com/avcenter/security/Content/2005.03.28.html>

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 two denial of service (DoS) issues identified in the AutoProtect functionality of the Symantec Norton AntiVirus consumer product. Where a real time scan of a specific file type can cause a system crash, Blue Screen of Death (BSOD), with both Symantec Norton AntiVirus 2004 and 2005 Windows applications. This type of file, while not malicious on its own, could be maliciously introduced either remotely from outside the system through email or over [http](http://), or internally by an authorized user to disrupt service on a targeted system.

Symantec product engineers confirmed both issues impacting Symantec's AutoProtect feature in Symantec Norton AntiVirus and have developed and released a patch for all impacted products through Symantec LiveUpdate. Customers

running Automatic LiveUpdate should already be updated. To manually update via Symantec LiveUpdate, users should run LiveUpdate until all available Symantec product updates are downloaded and installed.

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 1026 (----), 6346 (gnutella-svc), 1025 (----), 139 (netbios-ssn), 1027 (icq), 22321 (wnn6_Tw), 53 (domain), 80 (www) 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

27. *March 29, Associated Press* — **New fingerprint technology developed.** Scientists at the Los Alamos National Laboratory in New Mexico are using a new technique to see fingerprints on surfaces that typically make them invisible. The method uses a technology called mini-X-ray fluorescence to detect chemical elements in fingerprints without altering them, said Christopher Worley, a scientist on the project. The technology focuses a tight beam of X-rays on surfaces with fingerprints and creates a computer picture out of those scans. The equipment costs about \$175,000. The new method might also be able to tell if the person that left them handled certain types of bomb-making materials, said George Havrilla, another lab scientist. The technology for scanning the prints is widely available. What's new is the method the lab has created to see them -- which includes computer software and ways of manipulating the machinery, Worley said. But the technique isn't for everyone. "We've already had some negative comments on it," Havrilla said. "One reviewer told us it's just not practical. But the goal of our work was to demonstrate that it was feasible to see these things." The lab is interested in working with New Mexico police agencies to do more tests on the method, Worley added.

Source: <http://cnn.netscape.cnn.com/ns/news/story.jsp?id=200503291214001363668&dt=20050329121400&w=APO&coview=>

[[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:

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – 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. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

[Homeland Security Advisories and Information Bulletins](#) – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644 for more information.

Contact DHS/IAIP

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.

DHS/IAIP Disclaimer

The DHS/IAIP 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.