



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 13 November 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- Microsoft has released "Security Bulletin MS03–051: Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (Critical)," and a patch is available on the Microsoft Website. (See item [22](#))
- Microsoft has released "Security Bulletin MS03–048: Cumulative Security Update for Internet Explorer (Critical)," available on the Microsoft Website. (See item [24](#))
- Microsoft has released "Security Bulletin MS03–049: Buffer Overrun in the Workstation Service Could Allow Code Execution (Critical)," and a patch is available on the Microsoft Website. (See item [25](#))
- Microsoft has released "Security Bulletin MS03–050: Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run (Important)," and a patch is available on the Microsoft Website. (See item [26](#))

DHS/IAIP Update *Fast Jump*

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

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

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

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

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

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

Energy Sector

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

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

1. *November 11, Associated Press* — Secretary Abraham says Nevada nuke dump permit application will be on time. Energy Secretary Spencer Abraham said it won't be easy, but

the Department of Energy will file a license application for a Nevada nuclear waste repository by its goal of next December. Abraham said Monday, November 10, that a 2004 energy budget that Congress formed last week should contain enough money for the Energy Department to finish preparing a licensing package for the Yucca Mountain project. **Abraham said the Energy Department also needs enough money to develop a transportation program to ship radioactive spent fuel to the proposed repository 90 miles northwest of Las Vegas.** Last week, negotiators writing a new Energy Department spending bill settled on \$580 million for the Yucca Mountain Project next year. The amount was \$11 million less than what President Bush had requested, but several lawmakers said they were told it would be enough for the Energy Department to submit its license application to the Nuclear Regulatory Commission. The commission is expected to take three or four years to weigh the plan to begin entombing 77,000 tons of the nation's most radioactive commercial, industrial and military waste at the repository in 2010.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/news/archive/2003/11/11/state1151EST0031.DTL>

2. *November 10, Associated Press* — **Natural gas supplies adequate according to Energy Secretary. Natural gas inventories have rebounded and are above average for this time of year easing concern about possible tight supplies and price spikes this winter, Energy Secretary Spencer Abraham said Monday, November 10. Abraham said moderate weather has eased demand and allowed natural gas inventories to exceed levels they were last year at this time.** The Energy Information Administration said that 3.16 trillion cubic feet of natural gas were in storage at the end of October, just over one percent more than the five-year average. Last May, storage levels fell to the lowest ever recorded for the start of summer, nearly 40 percent below the five-year average, which prompted concern about natural gas supplies for this winter's heating season. However, summer weather was cooler than expected and this fall has been generally warmer, allowing the industry to build up supplies. **Residential consumers can still expect to pay more for heating this winter, compared to last year.** Much of the gas put in storage cost between \$5 and \$6 a thousand cubic feet on the wholesale spot market.

Source: http://story.news.yahoo.com/news?tmpl=story&u=/ap/20031111/ap_on_go_ca_st_pe/natural_gas_2

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

Chemical Sector

3. *November 12, Click On Detroit* — **Officials test air near Michigan chemical explosion. Crews from the Environmental Protection Agency (EPA) were called to the scene of a chemical explosion that happened in Brownstown Township Wednesday morning, Local 4 reported. The EPA was reportedly testing the air to make sure the area was safe. The explosion occurred around 6:30 a.m. inside the Chem Met Industries plant located on Allen Road, between Pennsylvania and Sibley roads, Local 4 learned. Two men were reportedly working with aluminum paste when there was a spark and an explosion, according to the station's reports. The men were not injured, but police say there was significant damage to the Chem Met building.** Wayne County road crews were ordered to block off both sides of Allen Road near the plant. Workers at the plant and at nearby businesses were reportedly waiting in a

store parking lot for officials to give clearance. Don Wells, a nearby business owner said it's not the first time this has happened. "It happened earlier in the summer ... there was a fire there, they shut down the road and had to evacuate everybody," said Wells. **EPA officials were awaiting the arrival of some equipment to complete their testing. Local 4 learned that the area may not be reopened for hours.**

Source: <http://cms.firehouse.com/content/article/article.jsp?id=sectionId=46&id=21700>

[[Return to top](#)]

Defense Industrial Base Sector

4. *November 12, Government Accounting Office* — **GAO-04-53: Defense Acquisitions: DoD's Revised Policy Emphasizes Best Practices, but More Controls Are Needed (Report).** The Department of Defense's (DoD) investment in new weapon systems is expected to exceed \$1 trillion from fiscal years 2003 to 2009. To reduce the risk of cost and schedule overruns, DoD revamped its acquisition policy in May 2003. The policy provides detailed guidance on how weapon systems acquisitions should be managed. The Senate report accompanying the National Defense Authorization Act for Fiscal Year 2004 required GAO to determine whether DoD's policy supports knowledge-based, evolutionary acquisitions and whether the policy provides the necessary controls for DoD to ensure successful outcomes, such as meeting cost and schedule goals. The report also required GAO to assess whether the policy is responsive to certain requirements in the Bob Stump National Defense Authorization Act for Fiscal Year 2003 concerning DoD's management of the acquisition process. **GAO recommends that the Secretary of Defense strengthen DoD's acquisition policy by requiring additional controls to ensure decision makers will follow a knowledge-based, evolutionary approach.** DoD partially concurred with GAO's recommendations. Report: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-53>
Source: <http://www.gao.gov/highlights/d0453high.pdf>

[[Return to top](#)]

Banking and Finance Sector

5. *November 12, CNETAsia* — **E-mail from 'Citibank' conceals Trojan.** An e-mail purporting to be from Citibank carries a Trojan virus that plants a back door on an infected computer, allowing a hacker to use the machine as a channel for other activities on the Internet. E-mail security company MessageLabs on Wednesday, November 12, reported the new e-mail virus, which has been dubbed Troj/Downloader!4c52 or **Downloader-DI.** The first copies of the e-mail have come from Australia, with more than 400 copies spotted so far, according to the company. The attachment is named www.citybankhomeloan.htm.pif. Once clicked, the Trojan attempts to download a further component from a free hosting Website located in Russia. After activation, this Trojan copies itself to the Windows System folder and installs a .DLL file, which enables the Trojan to act as a proxy server, allowing a hacker to channel Internet activities through the infected computer without the recipient's knowledge, according to MessageLabs.
Source: <http://news.zdnet.co.uk/business/0,39020645,39117827,00.htm>

6. *November 12, Taiwan News* — **Citibank investigates security breach for online credit cards. Citibank said on Tuesday, November 11, it was investigating a suspected information breach in its credit card application Web page, quickly assuring customers that its Internet banking service and existing client databases had not been compromised. The bank said it shut down all of its online application Web pages and online follow-up inquiry services on Tuesday after an applicant, Tsao Chih-cheng of the Wen Tzao Ursuling College of Modern Languages in Kaohsiung, Taiwan, reported that he could view the personal data information of other applicants.** Bank records showed that over 2,000 individuals had signed up for a Citibank credit card since an Internet campaign was launched on August 4, 2003, the bank said. The campaign allowed customers to apply for credit cards online. After filling out and submitting their basic information online, applicants still needed to download their filled out application forms and mail them to Citibank for review, the bank said. It added "The impact of this incident is limited to new online credit card applications only and does not involve any existing customer databases. Moreover, it will not affect in any way the rights of existing Citibank customers or the transactions made through its Internet banking service."
Source: <http://www.etaiwannews.com/Business/2003/11/12/1068600177.htm>

7. *November 12, CBC News* — **TD Canada Trust warns of e-mail scam. TD Canada Trust is warning its customers about an e-mail scam that tries to trick them into giving out their account numbers and PINs over the Internet. The bank said some of its customers have received e-mails that appear to be sent from TD, asking them for their personal information. The e-mail looks authentic and links to pages on the TD Canada Trust Website, but a pop-up box requesting account information actually sends that information to a server in Moscow.** TD Canada Trust spokesperson Jeff Key could not say whether any of the bank's customers have been taken in by the scam, but did say that TD is the fourth Canadian bank to be a target of phishing scams.
Source: http://www.cbc.ca/stories/2003/11/12/Consumers/td_email_scam_031112

8. *November 12, Dow Jones Newswires* — **U.S. Treasury freezes assets of alleged terrorists. The U.S. Treasury Department on Monday, November 10, designated 15 people as terrorists for involvement with al Qaeda cells in Italy. "According to documents provided by the Italian government, the 15 individuals have helped illegal immigration to Italy, and have provided financial and material support for terrorist activities in Italy and elsewhere in Europe,"** the U.S. Treasury said in a statement issued Wednesday, November 12. Some also recruited volunteers for military camps in Iraq, organized by the Ansar al Islam group, Treasury said. The cells were operating in Milan, Parma and Cremona. The Italian government, which has submitted the names of these people for designation by the U.N., has frozen their assets in Italy. Most of the 15 are being held by legal authorities. All have been charged with terror-related crimes in Italy, Treasury said. A list of the designated individuals is available on the U.S. Treasury Web site: <http://www.treas.gov>.
Source: http://biz.yahoo.com/djus/031112/1419001335_1.html

9. *November 11, Financial Times* — **Crime gangs extort money with hacking threat. Evidence of a new type of international extortion racket emerged on Tuesday, November 11, with revelations that blackmailers have been exploiting computer hacking techniques to**

threaten the ability of companies to conduct business online. Gangs based in Eastern Europe have been found to have been launching waves of attacks on corporate networks, costing the companies millions of dollars in lost business and exposing them to blackmail. The attacks involve gangs commandeering as many as hundreds of computers through hacking methods to use without their owners' knowledge. A command is then issued to each one simultaneously to make a series of bogus requests to the servers of the victim. The weight of traffic brings the servers to a halt and legitimate requests to carry out transactions cannot be completed. More than a dozen offshore gambling sites serving the U.S. market were hit by the so-called Distributed Denial of Service attacks and extortion demands in September and the tactic is now spreading. **Sites have been asked to pay up to \$50,000 to ensure they are free from attacks for a year. Police are urging any victims not to give in to blackmail and report the crime.**

Source: <http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1066565805264&p=1057562182635>

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

Transportation Sector

10. *November 12, Associated Press* — **All on board survive Illinois plane crash.** A commercial plane crashed Tuesday morning in a wooded area just south of Belleville, IL, but all four people on board survived, officials said. The St. Clair County Sheriff's Department received a report of the crash around 6:45 a.m., said Deputy Janet Bertelsman. **Volunteer firefighters, ambulances and rescue helicopters from St. Louis were at the scene, which Bertelsman said was "hard to get to because of the woods and the landscape." The plane was thought to be a Lear-type corporate jet.** Representatives of the Transportation Security Administration did not immediately respond to messages Tuesday.

Source: <http://www.newsday.com/news/nationworld/nation/wire/sns-ap-p-lane-crash.0.817965.story?coll=sns-ap-nation-headlines>

11. *November 12, Government Executive Magazine* — **TSA prepares for busy holiday season with reduced workforce. The Transportation Security Administration (TSA) expects longer wait times at airports this holiday season due to increased passenger traffic combined with a reduction in the number of passenger and baggage screeners, agency officials said last week.** "With the holiday travel season only weeks away, TSA is concerned at the increasing passenger flows we have been experiencing," Stephen McHale, TSA's deputy administrator, told the Senate Commerce, Science and Transportation Committee during a November 5 hearing. Under congressional orders, TSA reduced its screening workforce from 55,600 in March to 48,000 by the end of September. This Thanksgiving and Christmas will be the first major holidays TSA faces with the reduced workforce, while trends point to an increase in the number of airline passengers over last year. **McHale said TSA is launching a "large-scale public outreach effort" to educate passengers about what they can bring on planes, so screeners "are not distracted at security checkpoints by false alarms or items that passengers merely packed by mistake."** He said screeners have intercepted more than 1,500 firearms and more than 54,000 box cutters in the past year, and the number of intercepted prohibited items continues to rise.

Source: <http://www.govexec.com/dailyfed/1103/111103c1.htm>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

12. *November 12, Agricultural Research Service* — **ARS and Mexican research agency sign research agreement.** Officials from the Agricultural Research Service (ARS) and Mexico's National Council for Science and Technology (CONACyT) signed an agreement Wednesday expediting cooperative research to tackle agricultural problems affecting both the United States and Mexico. Under the agreement, ARS will work with CONACyT and Mexican agricultural research institutions to identify opportunities for ARS and Mexican scientists to collaborate on projects of mutual interest and benefit to both countries. **Wednesday's signing culminates more than a year's worth of activities in which representatives from more than a dozen Mexican research organizations and universities, ARS, other U.S. Department of Agriculture and federal agencies, and state universities participated in five workshops.** Their purpose was to identify agricultural research projects in areas that would improve trade for both countries. **The workshops focused on five main areas: agriculture's impact on water and the environment; food safety; pest problems, including phytosanitary issues; animal health; and plant biotechnology and biosafety.** Participants identified nearly 100 potential projects for cooperation, some of which have already started.

Source: <http://www.ars.usda.gov/is/pr/2003/031112.htm>

13. *November 12, Minnesota Ag Connection* — **Hunters' deer being tested for CWD. The opening of the Minnesota firearms deer season over the weekend also meant the start of a state effort to test for chronic wasting disease (CWD).** About 400 Minnesota Department of Natural Resources (DNR) staff and volunteers began collecting deer heads at more than 130 big game registration stations throughout the state. Testers remove a lymph node from the head for laboratory testing. DNR assistant wildlife chief Ed Boggess says the goal is to collect 13,000 samples from hunters this season. **Chronic wasting disease has not been found in Minnesota's deer population. Only two instances of the disease have been found in the state. Both were in farmed elk.**

Source: <http://www.Minnesotaagconnection.com/story-state.cfm?Id=998&yr=2003>

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

Food Sector

14. *November 11, Food and Drug Administration* — **Cheese recalled. Old Fashioned Foods in Mayville, WI, is voluntarily recalling snack cheese spreads and spreadable cream cheese that may be contaminated with Listeria monocytogenes bacteria, officials at the Wisconsin Department of Agriculture, Trade and Consumer Protection announced**

Tuesday. No illness has been reported to date in connection with the products. The products were distributed under the brand name Old Fashioned Cheese to retail stores throughout Wisconsin, in the Twin Cities area of Minnesota, and in the Rockford, IL, area. About 180 cases of the cheese spreads and 45 cases of the cream cheese were distributed. The potential contamination was found by Old Fashioned Foods' own testing program, which detected a positive result in one sample. **The company has ceased production and distribution of these products while they and the Wisconsin Department of Agriculture, Trade and Consumer Protection continue to investigate the cause of the problem.**

Source: http://www.fda.gov/oc/po/firmrecalls/mayville11_03.html

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

Water Sector

Nothing to report.

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

Public Health Sector

15. *November 12, Emory University Health Sciences Center* — Immune memory from smallpox vaccination. Immune memory after smallpox vaccination persists for at least 50 years in immunized individuals, according to research conducted by scientists at the Emory Vaccine Center and Emory University School of Medicine. Using a new blood test they developed to assess human antigen-specific immunity, the Emory scientists measured memory B cell responses in individuals recently vaccinated with smallpox vaccine, in unvaccinated individuals, and in individuals vaccinated between three months and 60 years earlier. The recently vaccinated group showed a significant virus-specific memory B cell response to vaccinia, while the unvaccinated individuals were negative for vaccinia virus-specific memory B cells. Vaccinia virus-specific B cells were detected in most of the previously vaccinated individuals in the study. The scientists found that virus-specific memory B cells initially declined after smallpox immunization, but then reached a plateau approximately ten times lower than their peak, where they remained stable for more than 50 years. **In addition, individuals vaccinated against smallpox maintained anti-smallpox antibodies in their blood for at least 60 years after vaccination, with no indication of decline.** In humoral immunity, the body's first line of defense against infection is antibodies produced by B cells, which are the primary measure of immunity for most vaccines.

Source: <http://www.sciencedaily.com/releases/2003/11/031112073642.htm>

16. *November 12, Financial Times* — WHO launches drive to stamp out fake drugs. A drive to stamp out the growing problem of substandard and counterfeit medicines in six south-east Asian countries is being launched this week by the World Health Organization (WHO). **Counterfeiting, mostly of antibiotics and drugs used to treat tuberculosis, malaria, and Aids, is widespread in Burma, Cambodia, China, Laos, Thailand, and Vietnam, the WHO says.** A meeting of the six countries, in Vietnam, is expected to agree on Friday on a series of joint activities to curb counterfeiting. **Figures are hard to come by but random testing of drug samples in Vietnam and Burma showed eight percent and 16 percent respectively**

were substandard, the WHO says. A study in south–east Asia in 2001 revealed that 38 percent of 104 antimalarial drugs on sale in pharmacies did not contain any active ingredients. **The WHO says counterfeiting is a worldwide industry worth more than \$32 billion in sales.** According to estimates by the U.S. Food and Drug Administration, counterfeits account for more than 10 per cent of the global medicines market while in poor countries up to a quarter of all medicines sold may be counterfeit.

Source: <http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1066565808258>

17. *November 11, Rocky Mountain News (Denver)* — **Chip to ID viruses. Researchers are working on a chip that could quickly determine whether a virus is inside a person. The chip would be able to identify a virus in an hour, helping health officials fight local epidemics or global pandemics, said researcher Kathy Rowlen,** a chemistry professor at the University of Colorado. In this era of worldwide air travel, an outbreak in central Africa can spell trouble in New York. That's why a rapid test to identify pathogens must be inexpensive and easy to manufacture, Rowlen said. Her team uses DNA microarrays to rapidly identify a virus based on its genetic signature. The DNA microarray is an arrangement of 27 micron–size spots on a microscope slide. Each microarray contains a layer of short strands of DNA from a known virus. A saliva or nasal sample from a person is cleaned and processed, made into a solution then exposed to the slide. If the virus is there, the genetic material will match up with the DNA already on the slide, revealing its presence, Rowlen said. **"It can screen for influenza A or B, or Severe Acute Respiratory Syndrome (SARS), or West Nile," said Rowlen, who predicts the chip will be in doctors' offices in two years. The chip should also be able to screen for other viruses, including engineered ones.**

Source: http://rockymountainnews.com/drmn/local/article/0.1299.DRMN15_2418902.00.html

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

Government Sector

18. *November 12, Federal Computer Week* — **Former intelligence officer joins DHS.** President Bush has tapped another former intelligence officer for a top job at the Homeland Security Department (DHS), as the agency works to gather and evaluate data to prevent another terrorist attack. **White House representatives said Bush plans to appoint Patrick Hughes as DHS' assistant secretary for information analysis.** Hughes was director of the Defense Intelligence Agency for more than three years. He also has been director of intelligence for the Joint Staff and the U.S. Central Command. He was the commanding general of the U.S. Army Intelligence Agency. He joins other top DHS officials who have experience in the intelligence field, including Frank Libutti, undersecretary of information analysis and infrastructure protection, and Robert Liscouski, assistant secretary for infrastructure protection.

Source: <http://www.fcw.com/fcw/articles/2003/1110/web-dhs-11-11-03.a.sp>

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

Emergency Services Sector

19. *November 12, Philadelphia Inquirer* — **Area readies for attack in practice run at refinery.** Led by the local U.S. Coast Guard unit, more than 300 emergency responders began a two-day exercise yesterday to simulate an oil spill caused by a terrorist attack, at the ConocoPhillips refinery in Delaware County, PA. It was a dress rehearsal to disaster, giving all the different players a chance to see how they would react to the situation and each other. A phony alert went out at 8 a.m. that Tank 181 at the ConocoPhillips refinery had collapsed. In the middle of the channel, workers on the hulking, 208-foot Delaware Responder skimmed the river's surface by maneuvering a 100-yard boom. **Meanwhile, a few miles away, teams of responders — from FBI agents to local police, state environmental officials, ConocoPhillips managers, emergency workers, and Coast Guard officers — set up a command center at the Embassy Suites near Philadelphia International Airport.** From there, they directed a two-pronged mission: containing the spill and investigating the terrorist strike. In the script of the exercise, **the ConocoPhillips refinery became a giant crime scene, with environmental protection officials from Pennsylvania, Delaware and New Jersey having to figure out how they would work elbow-to-elbow with criminal investigators.**
Source: <http://www.philly.com/mld/inquirer/news/local/7239078.htm>
20. *November 12, Business Wire* — **Chemical Biological Response Aide to coordinate response in upcoming regional New Jersey Gateway Response Exercise.** The Office for Domestic Preparedness (ODP), United States Department of Homeland Security (DHS), is field testing and evaluating CoBRA(R), a sophisticated emergency response system, to agencies participating in the New Jersey Gateway Response Exercise. **The Gateway Response is a series of exercises that will culminate in a full scale multi-jurisdictional exercise involving chemical and radiological weapons conducted at the Port of Newark on November 15, 2003.** Participating organizations will include local and county first responders, the New Jersey State responders, and federal agencies such as the FBI, and DHS Customs, Coast Guard and Federal Emergency Management Agency (FEMA). The CoBRA(R) systems, including software and ruggedized laptops, will be used by exercise participants, controllers and evaluators on site, where it will wirelessly make available critical information as well as automate the rapid and accurate collection of data during the course of the exercise.
Source: http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20031112005722&newsLang=en
21. *November 12, Transportation Security Administration* — **Deadline Extension – Interim Final Rule (IFR) for Hazardous Materials Endorsement .** The Transportation Security Administration (TSA) is amending its Interim Final Rule (IFR) that establishes standards for security threat assessments of individuals applying for, renewing, or transferring a hazardous materials endorsement (HME) for a commercial drivers license (CDL). **TSA is adding a definition and moving the date on which fingerprint-based criminal history record checks must begin to April 1, 2004.** If a State is unable to collect this information by April 1, 2004, the State must submit a request for extension to TSA on or before April 1, 2004.
Source: http://www.tsa.gov/public/display?theme=40&content=090005198_006440c

[[Return to top](#)]

Information and Telecommunications Sector

22. *November 13, Microsoft* — **Microsoft Security Bulletin MS03–051: Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution.** There are two vulnerabilities in Microsoft FrontPage Server Extensions. The first vulnerability exists because of a buffer overrun in the remote debug functionality of FrontPage Server Extensions. This functionality enables users to remotely connect to a server running FrontPage Server Extensions and remotely debug content using, for example, Visual Interdev. **An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause FrontPage Server Extensions to fail.** The attacker could then take any action on the system. The second vulnerability is a Denial of Service vulnerability that exists in the SmartHTML interpreter. This functionality is made up of a variety of dynamic link library files, and exists to support certain types of dynamic web content. **An attacker who successfully exploited this vulnerability could cause a server running Front Page Server Extensions to temporarily stop responding to requests.** Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.
Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03–051.asp>
23. *November 12, Government Accounting Office* — **GAO–04–55: Uneven Implementation of Wireless Enhanced 911 Raises Prospect of Piecemeal Availability for Years to Come (Report).** Enhanced 911 (E911) is in place in most of the country for traditional wireline telephone service, where the telephone number is linked to a street address. Expanding E911 capabilities to mobile phones is inherently more challenging because of the need to determine the caller's geographic location at the moment the call is made. **Concerns have been raised about the pace of wireless E911 implementation and whether this service will be available nationwide.** GAO reviewed the progress being made in implementing wireless E911 service, the factors affecting this progress, and the role of the federal government in facilitating the nationwide deployment of wireless E911 service. In order to provide the Congress and federal and state officials with an accurate assessment of the progress being made toward full deployment of wireless E911, **the GAO recommends that the Department of Transportation work with state officials and public safety groups to develop data identifying which public safety answering points (PSAPs) will need to have E911 equipment upgrades.** Highlights: <http://www.gao.gov/highlights/d0455high.pdf>
Source: <http://www.gao.gov/new.items/d0455.pdf>
24. *November 11, Microsoft* — **Microsoft Security Bulletin MS03–048: Cumulative Security Update for Internet Explorer. There are three vulnerabilities that involve the cross–domain security model of Internet Explorer, which keeps windows of different domains from sharing information.** These vulnerabilities could result in the execution of script in the My Computer zone. After the user has visited a malicious Website or viewed a malicious HTML e–mail message an attacker who exploited one of these vulnerabilities could access files on a user's system, and run arbitrary code on a user's system in the security context of the user. **Another vulnerability involves the way zone information is passed to an XML object within Internet Explorer.** This vulnerability could allow an attacker to read local files on a user's system. Finally, **there is a vulnerability that involves performing a drag–and–drop operation during dynamic HTML (DHTML) events in Internet Explorer.**

This vulnerability could allow a file to be saved in a target location on the user's system if the user clicks a link. No dialog box would request that the user approve this download. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install this patch immediately.

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-048.asp>

25. *November 11, Microsoft* — **Microsoft Security Bulletin MS03-049: Buffer Overrun in the Workstation Service Could Allow Code Execution. A security vulnerability exists in the Workstation service that could allow remote code execution on an affected system.** This vulnerability results because of an unchecked buffer in the Workstation service. If exploited, an attacker could gain System privileges on an affected system, or could cause the Workstation service to fail. **An attacker could take any action on the system**, including installing programs, viewing data, changing data, or deleting data, or creating new accounts with full privileges. If users have blocked inbound UDP ports 138, 139, 445 and TCP ports 138, 139, 445 by using a firewall an attacker would be prevented from sending messages to the Workstation service. Most firewalls, including Internet Connection Firewall in Windows XP, block these ports by default. Disabling the Workstation service will prevent the possibility of attack. Only Windows 2000 and Window XP are vulnerable to this attack. **Microsoft has assigned a risk rating of "Critical" to this issue** and recommends that system administrators install the patch immediately.

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-049.asp>

26. *November 11, Microsoft* — **Microsoft Security Bulletin MS03-050: Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run. A vulnerability exists in Microsoft Excel that could allow malicious code execution.** If successfully exploited, an attacker could craft a malicious file that could bypass the macro security model. If an affected spreadsheet was opened, this vulnerability could allow a malicious macro embedded in the file to be executed automatically, regardless of the level at which the macro security is set. The malicious macro could then take the same actions that the user had permissions to carry out. A vulnerability exists in Microsoft Word that could allow malicious code execution. If a specially crafted document were to be opened it could overflow a data value in Word and allow arbitrary code to be executed. If successfully exploited, an attacker could then take the same actions as the user had permissions to carry out. **Microsoft has assigned a risk rating of "Important" to this issue** and recommends that system administrators install this patch immediately.

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-050.asp>

Internet Alert Dashboard

| Current Alert Levels | |
|--|--|
|  AlertCon: 2 out of 4 https://gtoc.iss.net |  Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/ |
| Current Virus and Port Attacks | |
| Virus: | #1 Virus in the United States: WORM_LOVGATE.G Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States] |
| Top 10 Target Ports | 135 (epmap), 1434 (ms-sql-m), 137 (netbios-ns), 4899 (radmin), 445 (microsoft-ds), 80 (www), 139 (netbios-ssn), 1433 (ms-sql-s), 4444 (CrackDown), 57 (priv-term) Source: http://isc.incidents.org/top10.html ; Internet Storm Center |

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

General Sector

27. *November 12, Telegraph* — **Europe unveils agency to protect its borders.** Plans were unveiled yesterday for a pan-European border agency to help to seal the European Union's (EU) new frontier after expansion next year. **The agency is scheduled to start work in January 2005 with a \$4.6 million budget and a staff of 30. The Agency for the Management of Operational Co-operation at the External Borders will serve as a headquarters for air, sea, and land surveillance, keeping watch on Poland, Slovakia, and the Baltic states that will soon have the task of patrolling the EU's eastern borders.** Antonio Vitorino, the EU justice commissioner, said the staff would take instructions from an EU minister and would not be able to dictate strategic policy.
 Source: <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/11/12/wbord12.xml&sSheet=/news/2003/11/12/ixworld.html&secureRefresh=true&requestid=22654>
28. *November 12, Associated Press* — **Rain causes flooding in Ohio and West Virginia.** A band of heavy rain caused flooding Wednesday across a section of Ohio and West Virginia, closing schools and sending some people to higher ground. Up to two inches of rain fell across West Virginia, from Wood County on the Ohio River to Tucker in the northeast, the National Weather Service said. **Several people were evacuated near Boothsville, West Virginia because high water threatened their apartment building,** said Carolyn Ledsome of the Marion County emergency services office. The number of people involved immediately available, she said. **Schools were closed in four West Virginia counties and in three counties in southeastern Ohio, most because of water on roads in the hilly, largely rural region.** Several motorists needed help in West Virginia after driving onto water-covered sections of road. Rain also extended westward as far as Missouri and eastward through Maryland and New Jersey, with showers reaching the southern edge of New England.
 Source: <http://www.newsday.com/news/nationworld/nation/wire/sns-ap-f>

[loading.0.7506090.story?coll=sns-ap-nation-headlines](#)

29. November 07, U.S. Department of State — Public Announcement: Malaysia. The October 5, 2003, kidnapping of six Indonesian and Filipino workers from a resort along the coast of eastern Sabah reinforces the U.S. concern for the safety of travelers to that region of Malaysia. In 2000, armed gunmen associated with the terrorist Abu Sayyaf Group based in the southern Philippines took hostages from the islands of Sipadan and Pandanan in eastern Sabah and transported them to the Philippines. Since then, the Malaysian government has substantially increased its police and military presence in the region. Nonetheless, the region is large and remote and in many locations, which include open waters between the mainland and offshore resorts, emergency assistance may not always be available. In October 2002, the United States Government designated the Jemaah Islamiyah (JI) a Foreign Terrorist Organization. JI is an extremist group linked to al Qaeda and other regional terrorist groups and has cells operating throughout Southeast Asia. **Extremist groups in the region have demonstrated their capability to carry out transnational attacks in locations where Westerners congregate. Terrorist groups do not distinguish between official and civilian targets.**

Source: http://travel.state.gov/malaysia_announce.html

[[Return to top](#)]

DHS/IAIP Products & Contact Information

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

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

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

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

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

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

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov

or call 202-323-3204.

DHS/IAIP Disclaimer

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