



Media Advisory

October 2, 2002

Contact: Eleni Martin (202) 501-1231

GSA's Office of Citizen Services and Communications

The Top Twenty Internet Security Vulnerabilities for 2002

Plus A Three-Part Initiative To Find and Eliminate Those Vulnerabilities On Government and Private Systems.

The FBI's National Infrastructure Protection Center (NIPC), the U.S. General Services Administration's (GSA) Federal Computer Incident Response Center (FedCIRC) program, and the SANS Institute today announced the twenty vulnerabilities most often exploited by hackers and other cyber criminals. The Top Twenty has been updated substantially from last year – adding new vulnerabilities and removing some that are no longer prevalent. (Attachment 1 Lists the New Top Twenty Internet Security Vulnerabilities). A detailed description of the vulnerabilities and how to address them follows. (Attachment 2)

Simultaneously, four network scanner suppliers announced new releases of their products that allow clients to test for the Top Twenty (Attachment 3 provides brief summaries of the offerings of each of the vendors), and GSA's Federal Technology Service (FTS) announced that it is establishing a working group to draft task order specifications so federal agencies can use the GSA's SafeGuard contracting program to test for the Top Twenty vulnerabilities and to get help in removing them.

"This announcement raises awareness of the most critical vulnerabilities that affect everyone's information systems, said FTS Assistant Commissioner for Information Assurance and Critical Infrastructure Protection, Sallie McDonald. "Federal Government agencies should test their systems to determine whether any of the Top Twenty vulnerabilities are present. GSA's FTS can help agencies to procure industry experts to assist in the remediation process. This will go a long way to help prevent more serious computer security incidents. However, when vulnerabilities are exploited and incidents do occur, GSA's FedCIRC is ready to provide assistance."

This initiative guides federal agencies to replicate the ground-breaking work of the National Aeronautics and Space Administration (NASA) that demonstrated how to reduce the number of successful attacks using a comprehensive vulnerability testing and remediation program. Because the tools are equally available to non-governmental users, some available at no cost, all computer users can take advantage of the research and resources developed by the government, SANS and the security vendors.

Most importantly, this initiative establishes a measurable benchmark for Internet users and business partners to employ in requesting information about the security status of organizations they need to trust. Before providing a credit card to an Internet site, for example, it is not unreasonable to believe that consumers could ask for a certification that the site has been protected against the top twenty vulnerabilities.

Following the press announcement, representatives from the Government agencies and commercial companies will provide a briefing for 200 federal security and IT managers on the details of the initiative and how they use it to protect their computers.

For additional information contact the following:
CDR David Wray, NIPC public affairs, at 202-324-1284
Mary Alice Johnson, GSA public affairs, at 202-501-2699.

An International Partnership – Canada, the United States, the United Kingdom

The Canadian and British government organizations responsible for cyber security strategy issued a joint statement of support:

The NISCC (National Infrastructure Security Coordination Centre) in the United Kingdom and OCIPEP (the Office of Critical Infrastructure Protection and Emergency Preparedness) in Canada have both welcomed the US initiative to publish a list of the Top Twenty IT vulnerabilities. These two organizations are committed to working with their U.S. partners in raising awareness of the vulnerabilities in IT systems and the need to take appropriate remedial action to protect systems from electronic attack, both domestically and globally.

Both organizations issued Information Notes to their constituents timed to coincide with the US release of the new Top Twenty Internet Security Vulnerabilities.

For more information, the press may contact:

Canada's Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
E-mail: communications@ocipep-bpiepc.gc.ca
Phone: 1-800-830-3118

The United Kingdom's National Infrastructure Security Coordination Centre (NISCC)
enquiries@nisc.gov.uk

####