ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY OF PUBLIC WEB SERVERS

Shirley Radack, Editor, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Many organizations in industry, government, and academia use the Internet to publish and exchange information, serve their customers and the public, and conduct electronic transactions. The web server is the essential system component for providing these functions. The web browser is the corresponding software application on the user's computer. It accesses the information that is stored on web servers and displays it for the user. Both web servers and web browsers are vulnerable to malicious intruders, who can break into public websites, destroy or change information, and disrupt operations.

The National Institute of Standards and Technology (NIST) recently issued NIST Special Publication (SP) 800-44, *Guidelines on Securing Public Web Servers*, by Miles Tracy, Wayne Jansen, and Mark McLarnon, to help federal agencies improve the secure design, implementation, and operation of their web servers. These new guidelines complement NIST SP 800-46, *Security for Telecommuting and Broadband Communications*, which provides information for improved security of web browsers. Both publications were developed for the federal community, but should be useful to individuals, the private sector, and other public sector organizations.

NIST SP 800-44 describes secure practices for the installation and configuration of operating systems and web server software, and explains the use of devices such as firewalls, routers, switches, and intrusion detection systems to protect web servers. The publication also covers secure maintenance procedures and strategies for protecting information. The appendices provide details on the secure use of two popular web server applications: Apache Web Server and Microsoft Internet Information Server (IIS). Also included in the appendices are references available in print and electronic format, listings of web security resources, tools and applications, and useful checklists for web server security. Both NIST SP 800-44 and NIST SP 800-46 are available in electronic format from the NIST website: http://csrc.nist.gov/publications/nistpubs/index.html.

ITL's November 2002 bulletin summarized the recommendations and guidance in NIST SP 800-46. This and other bulletins issued by ITL are available at: http://csrc.nist.gov/publications/nistbul/index.html.

The Vulnerabilities of Web Servers

Because web servers are one of the few system components on a target network that typically communicates with untrusted third parties, they are frequently the targets of malicious attacks by intruders. Intruders can easily launch automated attacks against thousands of systems simultaneously to identify the relatively few vulnerable systems. New attacks can be set up and launched quickly from remote locations, foiling attempts by organizations to develop effective countermeasures. Once web servers have been compromised, the organization's other network resources are at greater risk. Intrusions can be very costly to the organization in terms of money, time, and damage to reputation. The confidentiality and/or integrity of the stored data can be jeopardized. Availability may also be affected, making the information on the organization's

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since June 2001

website effectively unobtainable. In addition, a compromised web server could be used to distribute illegally copied software, attack tools, and pornography or as a base from which to attack other networks, possibly exposing the organization to legal liability.

With good planning and rigorous implementation of secure configurations and operational procedures, organizations can operate successful websites while protecting their networks and information resources.

What Can Be Done To Protect Web Servers

Organizations need a security plan and a policy for implementing the plan, monitoring its effectiveness, and updating it. All those involved with or affected by the information processing systems have a role in protecting the security and the privacy of information assets. Security plans should include an overview of the security requirements of the system, the controls needed to meet those requirements, and the responsibilities of all individuals who access the system. With this basic planning as the foundation for secure systems, organizations should apply the following specific recommendations to improve the security of their web servers:

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

- **Plan carefully and address the security aspects of deployment of web servers.**

  Careful planning is essential before the installation, configuration, and deployment of web servers. It is more difficult to address security issues once deployment and implementation have been completed. A detailed and well-designed deployment plan facilitates the organization's decisions about tradeoffs between usability, performance, and risks. A deployment plan makes it possible to maintain secure configurations and to identify security vulnerabilities. The deployment plan should address:

  - The purpose of the web server, the information to be stored on or processed through the server, and the security requirements of the information and of related systems, networks, and services; and
  - The human resource requirements for the deployment and operational phases of web servers and their supporting infrastructures, including the types of personnel, their skills and training, and levels of effort required.

- **Implement appropriate security management practices and controls to maintain and operate a secure website.**

  Appropriate management practices are critical to operating and maintaining secure web servers. Organizations should identify their information system assets and determine the policies, standards, procedures, and guidelines that are needed to support the confidentiality, integrity, and availability of information system resources. All management controls that are required to protect information system assets should be developed, documented, and implemented.

  NIST recommends that organizations apply the following practices to ensure the security of web servers and their supporting network infrastructure:

  - An organization-wide information system security policy;
  - Configuration/change control and management;
  - Risk assessment and management;
  - Standardized software configurations that satisfy the information system security policy;
  - Security awareness and training;
  - Contingency planning, continuity of operations, and disaster recovery;
  - Certification and accreditation; and
  - Incident response policy and procedures.

- **Deploy, configure, and manage web server operating systems to meet the security requirements of the organization.**

  The first step in securing a web server is securing the underlying operating system. Most commonly available web servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems supporting the web servers are configured appropriately. The default hardware and software configurations of web servers may be set by vendors to emphasize features, functions, and ease of use, rather than the security of the system. Since each organization's security requirements are very different, web administrators should configure new servers to reflect their organization's security requirements. When these requirements change, the web servers should be reconfigured. The steps needed to secure the operating system include:

  - Patch and upgrade the operating system.
  - Remove or disable unnecessary services and applications.
  - Configure operating system user authentication.
  - Configure resource controls.
  - Test the security of the operating system.

- **Web server applications should be deployed, configured, and managed to meet the security requirements of the organization.**

  In many respects, the requirements for secure installation and configuration of web server applications are the same as for the operating systems. First and foremost, only the minimal and necessary portion of web server services should be installed. If vulnerabilities are identified, they should be eliminated through patches or upgrades. Unnecessary applications, services, and scripts should be removed immediately after the installation process has been completed. The steps that should be taken to secure the web server application include:

  - Patch and upgrade the web server application.
  - Remove or disable unnecessary services, applications, and sample content.
  - Configure web server user authentication.
  - Configure web server resource controls.
  - Test the security of the web server application and web content.

- Ensure that only appropriate content is published on the website and that the content is adequately protected from unauthorized alteration.

  Organizations should develop a web publishing process or a policy that determines what information may be published openly, what information may be published with restricted access, and what information should not be published in any publicly accessible repository. Websites are vulnerable to individuals who mine an organization's website in search of valuable information. In general, the following kinds of information should be carefully examined and reviewed before publication on a public website:

  - Classified information
  - Proprietary information
  - Information on the composition or preparation of hazardous materials or toxins
  - Sensitive information relating to homeland security
  - Detailed physical and information security safeguards
  - Details about network and information system infrastructure (e.g., address ranges, naming conventions, access numbers)
  - Information that specifies or implies physical security vulnerabilities
  - Detailed plans, maps, diagrams, aerial photographs, and architectural drawings of organizational buildings, properties, or installations.

- **Take appropriate steps to protect web content from unauthorized access or modification.**

  Organizations should control the information that is made available on public websites through their publishing processes or policies. Websites should be protected to assure that the information is not modified without authorization. Users rely on the integrity of the information made available to them. Because the information on public websites is easily accessible, it is more vulnerable to tampering and change than the information that is made available by the organization in other ways. Public web content must be protected through the appropriate configuration of web server resource controls. Some of the resource control practices that should be applied include:

  - Install or enable only necessary services.
  - Install web content on a dedicated hard drive or logical partition.
  - Limit uploads to directories that are not readable by the web server.
  - Define a single directory for all external scripts or programs executed as part of web content.
  - Disable the use of hard or symbolic links.
  - Define a complete web content access matrix to identify the folders and files within the web server document directory that are restricted and those that are accessible. People who have access to both the restricted and accessible folders and files should be identified.
  - Disable directory listings.
  - Use user authentication, digital signatures, and other cryptographic mechanisms as appropriate.
  - Use host-based intrusion detection systems and/or file integrity checkers to detect intrusions and verify web content.

- **Active content should be used only after careful consideration of the benefits to be gained and the associated risks.**

  Interactive elements, supported by technologies such as ActiveX, Java, VBScript, and JavaScript, enable users to interact with websites in new ways. No longer confined just to accessing text-based documents, users can carry out a wide range of applications. These interactive elements introduce new web-related vulnerabilities since they involve moving code from a web server to a client application for execution. Users are at risk because active content can take actions on the user's computer without the permission or knowledge of the user. Content generation technologies on the web server pose a similar risk because, when accepting input from users,

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

they may be induced to take actions that could harm the server. One such risk is accepting large amounts of information that can overflow buffers and be used to execute commands or gain unauthorized access to the web server. All content must be protected, and close attention should be given to proper programming of browsers and servers. The different active content technologies have different vulnerabilities associated with them, and all must be carefully considered to balance benefits and risks.

- **Authentication and cryptographic technologies should be used appropriately to protect certain types of sensitive data.**

  Organizations should examine all of the information available on their public web servers and determine their requirements to protect the integrity and confidentiality of that information. Web servers can support a range of authentication and encryption technologies, which can be used to identify and authenticate users with different privileges for accessing information. Using appropriate user authentication techniques, organizations can selectively restrict access to specific information. Otherwise, all information on a public web server could be accessed by anyone with access to the server. Certain user authentication processes protect the user as well by enabling the user to verify the server being accessed is the "authentic" web server and not a counterfeit version operated by a malicious entity.

  Technologies based on cryptographic functions can provide an encrypted channel between a web browser client and a web server that supports encryption. Web servers may be configured to use different cryptographic algorithms, providing varying levels of security and performance.

- **Use the network infrastructure to help protect public web servers.**

  The network infrastructure that supports the web server plays a significant role in the security of the web server. With careful configuration and deployment, the network infrastructure can be used to protect the public web server. Network design is influenced by factors such as cost, performance, and reliability, as well as by security. But network design alone cannot protect a web server. The frequency, sophistication, and variety of web attacks carried out today reinforce the need for layered and diverse defense mechanisms. Some of these defense-in-depth mechanisms include selection of a relatively safe network on which the public web server will be located and configuration of the network to support and protect the web server.

- **An ongoing process must be used to maintain the continued security of public web servers.**

  Maintaining a secure web server requires constant effort, resources, and vigilance. After a web server has been deployed, web administrators must monitor it on a daily basis to assure the continuing level of security. The following steps are essential to maintaining the security of a web server:

  - Configuring, protecting, and analyzing log files;
  - Backing up critical information frequently;
  - Maintaining a protected authoritative copy of the organization's web content;
  - Establishing and following procedures for recovering from compromise;
  - Testing and applying patches in a timely manner; and
  - Testing security periodically.

Summary

Organizations and users benefit when access to public web servers is safe and convenient and when the organization's electronic information resources are secure, reliable, and available. As is the case with all other aspects of remote access to organizational resources, the use of public web servers entails risks as well as benefits. These risks and benefits must be managed through careful planning and through implementation of guidelines for secure operation of public web servers.

Supplemental Information

Under the Computer Security Act of 1987 (P.L. 100-235), the Computer Security Division of the Information Technology Laboratory (ITL) develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, network security, criteria and assurance, and security management and support.

NIST issues publications covering research, guidance, standards, and the results of collaborative outreach efforts with industry, government, and academic organizations. NIST publications dealing with information security topics, including archived copies of bulletins, are available in electronic format from the NIST Computer Security Resource Center at: http://csrc.nist.gov/publications/.

Reference List

NIST Special Publications provide guidance and help organizations establish a foundation for good security practices. Some of these publications are:

- NIST Special Publication 800-3, *Establishing a Computer Security Incident Response Capability*, November 1991
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998
- NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001
- NIST Special Publication 800-27, *Engineering Principles for Information Technology Security,* June 2001
- NIST Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001
- NIST Special Publication, 800-31, *Intrusion Detection Systems (IDS)*, November 2001

- NIST Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001
- NIST Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001
- NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002
- NIST Special Publication 800-40, *Procedures for Handling Security Patches*, September 2002
- NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002
- NIST Special Publication 800-42, *Guideline on Network Security Testing*, draft
- NIST Special Publication 800-43, *Guide to Securing Windows 2000 Professional*, November 2002
- NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002
- NIST Special Publication 800-45, *Guidelines on Electronic Mail Security*, September 2002
- NIST Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, September 2002
- NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002
- NIST Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002
- NIST Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002
- NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*, draft.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900