ARCHIVED PUBLICATION

The attached ITL Bulletin is provided here only for historical purposes.

Any mention of the ICAT website or URLs to the ICAT Metabase, the ICAT Metabase has been renamed to the National Vulnerability Database (NVD), http://nvd.nist.gov/. The NVD website is hosted by NIST's Computer Security Division.

For current information on NIST's computer security publications and activities, please see the ITL Bulletins available on the Computer Security Division's website, http://csrc.nist.gov/publications/PubsITLSB.html.

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

IDENTIFYING CRITICAL PATCHES WITH ICAT

By Peter Mell
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Introduction to ICAT

Recent attacks on computer systems have intensified the need for relevant, timely information about the attacks and how to prevent them. The Computer Security Division at NIST's Information Technology Laboratory has created a searchable index containing 700 of the most important publicly known computer security vulnerabilities. This index, called ICAT (pronounced eye-cat), helps the user to search for specific vulnerabilities and identify those vulnerabilities that are applicable to their organizations. ICAT provides a summary of selected vulnerabilities and links to patch information specific to each vulnerability. ICAT is available at: http://csrc.nist.gov/icat. Organizations are advised to use a tool such as ICAT to find and fix the vulnerabilities in their networks.

ICAT enables systems administrators to find patches for a particular system, but it does not provide a general methodology for applying patches in an organization. This *ITL Bulletin* presents such guidance. ICAT will be most effective when applied using the suggested methodology.

The Common Vulnerabilities and Exposures List

The vulnerability information indexed by ICAT pertains to those vulnerabilities included in a standard vulnerability-naming scheme called CVE (Common Vulnerabilities and Exposures). The CVE standard defines a unique name for every widely applicable vulnerability. The list of vulnerability names and information on CVE is maintained by MITRE and can be viewed at: http://cve.mitre.org. The vulnerabilities in the CVE list are chosen by a prominent board of industry, government, and academia members (http://cve.mitre.org/Board_Sponsors/board.html) from the set of vulnerabilities publicly announced on the Internet. While this board's mission is to uniquely name all publicly known vulnerabilities, they are currently targeting recently discovered vulnerabilities and older vulnerabilities that are important enough to be included in commercial intrusion detection and vulnerability scanning products.

By leveraging the knowledge and experience of the CVE board, ICAT contains a set of vulnerabilities that are among the most significant. It is important that organizations defend themselves against each one of these vulnerabilities. Since the current list of 700 vulnerabilities is too large for system administrators to manually review, we created ICAT to allow one to search for vulnerabilities applicable to a particular organization's hosts.

Uses of ICAT

ICAT can help secure a network in a variety of ways, such as the following:

Securing a Host with ICAT

System administrators can use ICAT to find the vulnerabilities in their systems and to find relevant patches that will secure their systems. There are four steps in using ICAT:

■ Identify the names and version numbers of any software running on the host (e.g., Solaris 2.5). Of particular importance is the operating system and server software.

■ Search ICAT for the vulnerabilities that are applicable to the identified set of software. (See below for instructions on searching ICAT.)

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 January 1999

- *Secure Web-based Access to High Performance Computing Resources*, January 1999
- *Enhancements to Data Encryption and Digital Signature Federal Standards*, February 1999
- *Measurement and Standards for Computational Science and Engineering*, March 1999
- *Guide for Developing Security Plans for Information Technology Systems*, April 1999
- *Computer Attacks: What They Are and How to Defend Against Them*, May 1999
- *The Advanced Encryption Standard: A Status Report*, August 1999
- *Securing Web Servers*, September 1999
- *Acquiring and Deploying Intrusion Detection Systems*, November 1999
- *Operating System Security: Adding to the Arsenal of Security Techniques*, December 1999
- *Guideline for Implementing Cryptography in the Federal Government*, February 2000
- *Security Implications of Active Content*, March 2000
- *Mitigating Emerging Hacker Threats*, June 2000

■ Use the ICAT search filters to identify the most dangerous vulnerabilities that exist in the system. These problems should be fixed immediately.

■ Use the ICAT vulnerability summary pages to find links to relevant patch and vulnerability information.

Evaluating a Penetrated System with ICAT

When a host is penetrated and the penetration discovered, ICAT can aid system administrators and incident response teams by identifying methods by which a hacker could have entered the host. The related vulnerability entries in ICAT reveal what type of control the attacker could have gained over the machine. Such information can be very useful in restoring a penetrated host.

As with any crime, whenever a computer is penetrated, contact the appropriate legal and investigatory authorities. Also, government-sponsored incident response teams are available to assist in recovering from an attack. Government civilian agencies should contact the Federal Incident Response Capability (FedCIRC) at http://www.fedcirc.gov. Commercial organizations may contact the Carnegie Mellon Computer Emergency Response Team/Coordination Center (CERT/CC) at http://www.cert.org.

Understanding the Output of Security Products

An increasing number of security products identify vulnerabilities and attacks using CVE standard names. Since it uses CVE names, ICAT can be used to research the vulnerabilities and attacks reported by intrusion detection systems and vulnerability scanners. A list of over 25 vendors and computer security organizations using the CVE vulnerability-naming scheme is available at: http://cve.mitre.org/About_CVE/About/othersites.html.

Searching ICAT

ICAT's Web-based interface, shown in Figure 1, is easy to use and is well documented on the Web site. In this section, we present a short introduction to and an example of the ICAT search capability. We suggest that you follow this example on the ICAT Web site.

At the ICAT search page, type in a keyword associated with the type of vulnerabilities that you wish to view. Type in the names of software products, operating systems, or devices. For example, type "solaris." To see only entries containing a particular keyword, type "+" before the word. For example, to see only vulnerabilities pertaining to Solaris systems, enter "+solaris." Include software version numbers to further refine a search. Enter "+solaris 2.5" (note the necessary space between keywords). The resulting search will list all Solaris vulnerabilities with those pertaining to version 2.5 at the top of the list. Avoid uppercase letters when searching ICAT, as that will result in a case-sensitive search.

At this point, type “+solaris 2.5” into the search text string box and press the

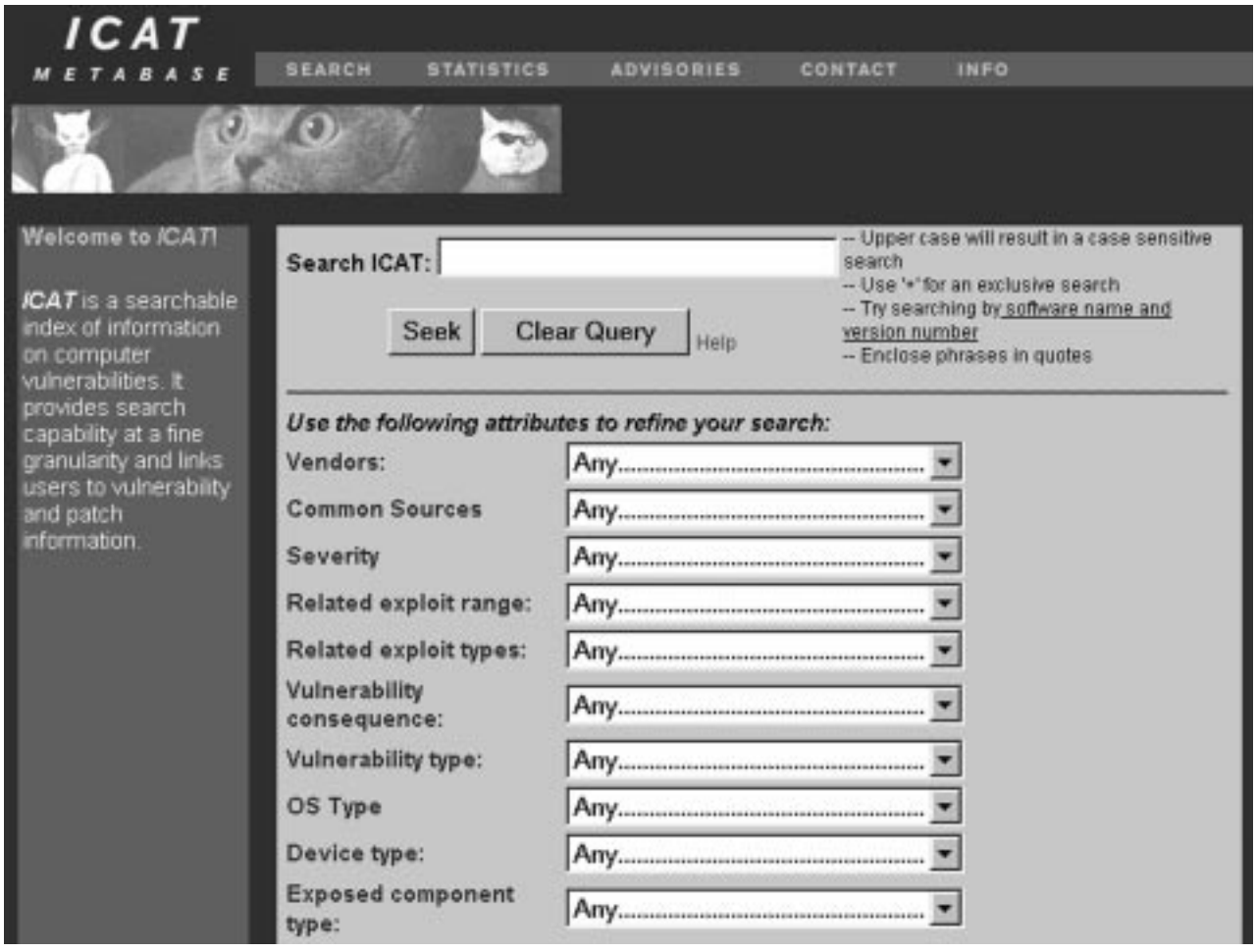

Figure 1: ICAT search page

Severity: High severity Medium severity Low severity	**Exploit range:** Local Remote	**Common sources:** CERT ISS X-Force Security focus
Related Exploit Types: Denial of service Penetration attacks	**Vulnerability Consequence:** Availability (impede host operation) (impede service operation) Confidentiality Integrity Security protection (gain superuser access) (gain user access)	**Vulnerability Type:** Input validation error (boundary condition error) (buffer overflow) Access validation error Exceptional condition error Environmental error Configuration error Race condition
OS type: Unix Windows 98 line Windows 2000 line Apple	**Device type:** Server Workstation Networking/security Other device type	**Exposed component type:** Operating system Network protocol stack User application Server application Hardware Communication protocol Encryption module Other type of component

Table 1: Search filters available in the ICAT drop-down search menus

"Seek" button. ICAT will return at least 98 vulnerabilities that are applicable to version 2.5 of the Solaris operating system. Before we discuss the search-results page, press the browser back button and we will refine our search using the drop-down menus. At this point, you should have "+solaris 2.5" typed into the search text box and all drop-down menus should be set to "Any."

Use the drop-down menus to refine your search. Each menu permits the user to choose a particular vulnerability attribute. The search engine returns only vulnerabilities that meet the criteria specified in ALL drop-down menu selections. Most of the available drop-down menus and associated choices are shown in Table 1. (See the ICAT documentation for an explanation of the terms in Table 1.)

Besides the drop-down menus listed in Table 1, there is also a menu to search the vulnerability entries by vendor names. There are currently 77 vendors represented in the ICAT vulnerability set.

At this point, we will refine our current query using the drop-down menus. Using the "Related exploit range" menu, select "Remote" to specify that we want to view only remotely exploitable vulnerabilities. Also, using the "Severity" menu, select "High severity" to specify that we want to look only at vulnerabilities that meet ICAT's definition of high severity (see the documentation for details).

A Sample ICAT Entry

After creating a search query, press the "Seek" button and ICAT will state the number of search results and a list of vulnerabilities that meet the search criteria. Each vulnerability is identified by a CVE number, a one-line description, and the date on which the vulnerability was first published. Browse through the vulnerabilities and click on "CVE 1999-0210."

As shown in Figure 2, you are now presented with an ICAT entry that summarizes the vulnerability. The entry is not a complete description of the vulnerability because ICAT is not a vulnerability database. Instead, ICAT summarizes the most important features of the vulnerability. This will enable you to quickly determine whether the vulnerability is applicable to your environment. Several fields will be particularly useful:

- the "Summary" line gives a one-line description of the vulnerability,
- the "Vulnerable software and versions" line lists the name and version numbers of the vulnerable software,
- the "Applicable vendors" line lists the vendors whose software is vulnerable to this problem,
- the "Exploitable Range" line tells whether or not a vulnerability can be remotely exploitable, and
- the "Loss type" line describes what kind of privilege the vulnerability can give a hacker.

If the vulnerability is applicable, one will need to find patch information and a more thorough description of the vulnerability. To fulfill this need, ICAT provides one or more references to patch sites or vulnerability database entries that contain more information. Continuing with our example, click on

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.

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 Web site is http://www.itl.nist.gov/.

the hyperlink in the row labeled "Reference 2." This link takes one to the CERT/CC advisory Web site and looks up the particular vulnerability. The CERT/CC advisory thoroughly describes the vulnerability and provides patch information. When you are done browsing the CERT advisory, press the search button on the top menu bar to return to the ICAT search screen.

The Importance of Security Advisories

While ICAT will aid system administrators by identifying recent vulnerabilities, it is not an early warning system. However, it is important that every organization subscribe to an early warning service. To understand why this is necessary, consider what happens when a hacker publishes a widely applicable attack script on the Internet. Overnight, millions of systems can become completely vulnerable to anyone running the script. In such cases, organizations must be notified very quickly.

Several incident response teams send out early warning advisories along with advisories about high-impact vulnerabilities. The advisories describe the vulnerability and how to mitigate or patch the problem. Every organization should monitor these advisories and have a program in place to take appropriate action. Most incident response teams have a mailing list so that new advisories are automatically sent to the appropriate person. Two of the best sources for such advisories are FedCIRC and the CERT/CC.

While important, advisories cover only the most critical vulnerabilities. Consequently, monitoring these advisories is not sufficient. Advisories must be used in conjunction with another tool, such as ICAT, that covers a broader range of known vulnerabilities.

Guidance on Patching Systems

Updating software is one of the most important aspects of maintaining a secure network. It is often overlooked because it seems like a monumental task. For example, how can a single system administrator spend several hours updating each computer at a site with 500 computers? While updating the computers in your network seems overwhelming, this section provides guidance on updating software efficiently. We assume that organizations will be manually installing patches, as this is the most common method today. However, new software is coming to market that allows one to automatically distribute patches throughout an enterprise.

Types of Patches

Patches are small programs that replace error-ridden code with corrected code. The term "patching" is used to refer to fixing security flaws in

Vulnerability Name:	CVE-1999-0210
Published before:	11/26/97
Summary:	Automount daemon automountd allows local or remote users to gain privileges via shell metacharacters
Severity:	High severity
Vulnerability type:	Access validation error
Exploitable Range:	Remote, Local
Loss type:	Security Protection (Gain superuser access) (Gain user access)
Exposed system component:	Operating system (automountd)
Exposed system type:	Server (Unix)
Reference 1:	Source: Security Focus Type: General and Patch Name: bugtraq id 235 http://securityfocus.com/bid/235
Reference 2:	Source: CERT Type: General and Patch Name: CA-99-05 http://www.cert.org/advisories/CA-99-05-statd-automountd.html
Applicable vendors:	Sun
Vulnerable software and versions:	Sun Solaris 2.5.1_x86 Sun Solaris 2.5.1 Sun Solaris 2.5_x86 Sun Solaris 2.5 Sun Solaris 2.4_x86 Sun Solaris 2.4

Figure 2: Typical ICAT vulnerability entry

software. There are three ways to fix security flaws or to "patch a system": work-arounds, patches, and upgrades. Work-arounds are procedures that a system administrator can use to fix a vulnerability. However, applying work-arounds may limit the functionality of the system being protected. While people generally talk about patching a system to secure it, upgrading to the newest software version is often, but not always, a simple way to ensure that all relevant patches are installed.

Three Steps to Patching a Network

Step 1: *Identify Critical Resources*

Identify those computers in your network that are critical and update those first. Critical hosts are typically those that are most visible to the outside world, those that store mission-critical data, and those that provide the most critical resources. A typical network's list of critical resources includes external Web sites, routers, firewalls, e-mail servers, DNS servers, and database servers.

Step 2: *Updating Critical Resources*

Each critical host should be examined regularly (at least monthly) to determine if any software needs to be updated. All software that an attacker could exploit must be updated regularly. Software in this category includes the operating system, servers or any software that receives network packets, software running as root or administrator, and security software (especially virus checkers). Make a list of such software per host and write down the associated version numbers. Then, find and install the available patches that are to be applied to your version of the software by using ICAT or by visiting the patch site of each vendor for every software package on a host. Each software vendor will have unique instructions on how to install their patches. Be careful to follow their instructions, as patches sometimes must be installed in a strict sequence for the process to work.

Step 3: *Updating Non-Critical Resources*

Non-critical hosts are obviously less important to protect than critical hosts. However, an attacker may break into a non-critical host and then use that host to attack critical resources. Thus, the level of security of non-critical hosts is important. Since it is a daunting task to update the software on all non-critical hosts in a network, many systems administrators do not regularly update non-critical hosts that are shielded with external and internal firewalls. The firewalls prevent outside network traffic from being routed to non-critical hosts, which helps protect them from attack. This technique works well but it does not protect against all attacks. Specifically, viruses and Trojan horses (especially those transmitted through e-mail that are typically passed through the firewall) can still attack non-critical hosts.

In order to secure non-critical hosts cost-effectively, install firewalls inside your organization to protect groups of non-critical hosts from other parts of the network. This way, if an attacker breaks into a host in your organization, the attacker cannot easily spread their influence to other hosts. Install virus checkers on all non-critical hosts that receive e-mail and configure them to automatically update weekly, if not daily. Lastly, once every year update each non-critical host as defined in step 2. If possible, use a standard configuration for non-critical systems, as this will simplify patching efforts.

Life for systems administrators will be made easier if users are trained to perform simple updates on their own machine. For example, users can be trained to periodically use the Microsoft® "Windows® Update" page to automatically fix security holes in the majority of non-critical host operating systems. Also, systems administrators can advertise that new versions of popular software are available for download. More advanced users will download the new version to get better features and will, as a result, install the latest security patches.

Maintaining Patch Records

We recommend that every organization maintain a Web server containing all patches they want applied to their software. This enables systems administrators to determine which patches have been approved by their organization. Records should be kept on the software and version numbers on all critical systems as well as which patches have been applied.

Automated Patch Dissemination Technology

Enterprise management systems are now becoming available that will automatically patch a set of hosts given commands from a single console. Such technology greatly reduces the time involved in installing patches and will greatly enhance the security of organizations using it. However, some organizations may prefer to wait before using this technology as the available solutions are still emerging technologies.

Conclusion

The ICAT Metabase is a tool that enables one to quickly identify the vulnerabilities that may exist in their systems. ICAT also provides links to relevant patch information. It provides a fine granularity of searching while covering a much larger set of vulnerabilities than is covered by most security advisories. ICAT informs administrators of the most serious threats and enables them to focus patching efforts on those patches that provide the greatest increases in security. ICAT can be an effective tool for improving the security of hosts on a network.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology 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

Official Business
Penalty for Private Use $300

Address Service Requested