netVigilance

ScoutNews Team
Issue #7

Weekly ScoutNews by netVigilance

Table of Contents

This Week In Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

This Week in Review

"May you live in interesting times" goes the old curse. Times are interesting indeed in the world of computer security, especially this week. Windows 2000 and NT source code leaked and spreading; a 'Robin Hood' virus trying to save us from MyDoom and the Microsoft ASN.1 Library vulnerability patch was released. No lack of things to pay attention to is there?

Today is Friday the 13th. It will be unlucky only if you didn't patch your network or run a scan for vulnerabilities.

15 day Trial. If for some reason you are reading this and haven't tried **SecureScout NX**, you are in luck. In many places in the world, you can now sign up to try SecureScout NX for free on 15 IP addresses for 15 days. http://www.netvigilance.com/trial

Top Security News Stories this Week

❖ Microsoft Warns of Widespread Windows Flaw

Microsoft has a message for Windows users: Patch your computers quickly. On Tuesday, the software giant released a fix for a networking flaw that affects every computer running Windows NT, Windows 2000, Windows XP or Windows Server 2003. If left unpatched, the security hole could allow a worm to spread quickly throughout the Internet, causing an incident similar to the MSBlast attack last summer. ...

http://news.com.com/2100-7355-5156647.html
By Robert Lemos – CNET

What You Should Know About the Windows Security Updates for February 2004
http://www.microsoft.com/security/security_bulletins/20040210_windows.asp

Microsoft Security Bulletin MS04-007 ASN.1 Vulnerability Could Allow Code Execution (828028)
http://www.microsoft.com/technet/security/bulletin/MS04-007.asp

Microsoft Security Bulletin MS04-006 Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution (830352) http://www.microsoft.com/technet/security/bulletin/MS04-006.asp

Microsoft Security Bulletin MS04-004 Cumulative Security Update for Internet Explorer (832894) http://www.microsoft.com/technet/security/bulletin/MS04-004.asp

❖ Gone Phishing

Phishing attacks involve the mass distribution of 'spoofed' e-mail messages with return addresses, links, and branding which appear to come from banks, insurance agencies, retailers or credit card companies. These fraudulent messages are designed to fool the recipients into divulging personal authentication data such as account usernames and passwords, credit card numbers, social security numbers, etc. Because these emails look “official”, up to 20% of recipients may respond to them, resulting in financial losses, identity theft, and other fraudulent activity. Visit one of the better web sites on this subject to find out more. http://anti-phishing.org

Also read Andrew Rose’s opposition to the anti-phishing SPF at http://catless.ncl.ac.uk/go/risks/23/18/10

http://www.vnunet.com/News/1152405’
By Robert Jaques - Vnunet

❖ Cisco Develops WLAN Security Protocol to Defeat Password Attacks

Cisco Systems Inc. has developed a new wireless LAN security protocol designed to defeat brute force dictionary attacks that capture a user's passwords, and it submitted a draft of the protocol to the Internet Engineering Task Force (IETF) on Monday. The fix will be available by the end of March. Cisco developed the new WLAN Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) to defeat dictionary attacks against unencrypted passwords in its earlier, proprietary Lightweight Extensible Authentication Protocol (LEAP). Cisco posted a security bulletin last August warning users that LEAP is vulnerable to such attacks (see story).

http://www.computerworld.com/securitytopics/security/story/0,10801,90163,00.html
By Bob Brewin – Computerworld

❖ Automating Windows Patch Management

Patch management could easily be called the bane of every administrator's existence, the pain in the rear of system management, or that never ceasing headache that pounds at CIOs everywhere. And I use the term "management" loosely. As I write this there are more than 40 updates that need to be applied to a new Dell computer running Windows XP. There were over 20 updates for Windows 2000 Service Pack 3 to apply to new systems before Microsoft released the fourth service pack in the summer of 2003. With this ever-growing hairball of security fixes, bug fixes, critical updates, and patches, might it be easier to disconnect all machines from the Internet and work with stone tablets than deploy new systems? But that's not feasible, of course. As things stand now, there are a few ways to handle distributing and applying updates:

- the sneakernet way;

- using Microsoft-sanctioned mechanisms; or
- investing money in third-party patch distribution systems.

In this article, I'll discuss Microsoft's Software Update Services (SUS) in depth, including installation, administration, and maintenance. I'll also look at freeware and commercial alternatives to patch management and why certain solutions might-or might not-be the best fit for your enterprise.

http://www.securityfocus.com/infocus/1760
By Jonathan Hassell - SecurityFocus

❖ New Virus Picks Fight with MyDoom. Nachi.B Tries to Undo MyDoom Damage

Seems hardly a day goes by that you don't hear about one virus or another lately. A new virus has been released this week which attempts to undo the damage caused by MyDoom. Of course you may remember a virus called Nachi-A which was released back in August 2003. Nachi-A was launched in a vain attempt to cure machines infected with the Blaster virus. It would do this by deleting all files relating to the virus and then automatically downloading security patches from the Microsoft website. Well, Nachi is up to it's old tricks again. Nachi-B has been released today in yet another vain attempt to clear up the mess made by the MyDoom worm over the last few weeks. In an interesting turn, this new variant of Nachi is apparently sending a political message to computers running Japanese versions of Windows. The dates appear to coincide with when Japan engaged in some kind of aggression against China.

http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/50337246?-2622
http://www.silicon.com/networks/webwatch/0,39024667,39118388,00.htm
By Tech Staff – Sophos / Dawn Kawamoto - Silicon

New Vulnerabilities Tested in SecureScout

Eight new vulnerability Test Cases have been incorporated into the SecureScout database this week including a test for the ANS 1 Library patch! Of course, these weekly updates are what keeps your network scanning tool one step in front of the hackers, inside or outside the organization.

➢ 12102 64k Rule Based TCP ISN Vulnerability

It is possible to spoof legitimate users to establish connections to your host. When opening a connection on a TCP port, an Initial Sequence Number (ISN) is given. If the ISN can be guessed, it makes it easy for an attacker to establish a connection spoofing a legitimate user. This could give access to services that should not be reachable by any outsider. This test case checks if the ISN is based on the 64k Rule. 64k Rule : The Berkeley implementation (and all derivatives) increment the ISN clock by 128,000 each second and by a further 64,000 for each new connection.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **Low**

CVE Link: No CVE link available
References: http://www.ietf.org/rfc/rfc1948.txt
http://www.ietf.org/rfc/rfc793.txt

- **14398 Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution**

  A security vulnerability exists in the Windows Internet Naming Service (WINS). This vulnerability exists because of the method that WINS uses to validate the length of specially-crafted packets. On Windows Server 2003 this vulnerability could allow an attacker who sent a series of specially-crafted packets to a WINS server to cause the service to fail. Most likely, this could cause a denial of service, and the service would have to be manually restarted to restore functionality. On Windows NT and Windows 2000, the nature of the vulnerability is slightly different. WINS will reject the specially-crafted packet and the attack does not result in a denial of service. The vulnerability on these platforms also does not allow code execution. Microsoft is releasing a security update for these platforms that corrects the vulnerable code as a preventive measure to help protect these platforms in case methods are found in the future to exploit this vulnerability.

  Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **High**

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0825
  Microsoft:
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms04-006.asp

- **14399 ASN.1 Vulnerability Could Allow Code Execution (MS04-007/828028)**

  This vulnerability may be one of the most important you have ever patched. We have a test for it. As you have heard, a security vulnerability exists in the Microsoft ASN.1 Library that could allow code execution on an affected system. The vulnerability is caused by an unchecked buffer in the Microsoft ASN.1 Library, which could result in a buffer overflow. An attacker who successfully exploited this buffer overflow vulnerability could execute code with system privileges on an affected system. The attacker could then take any action on the system, including installing programs, viewing data, changing data, deleting data, or creating new accounts with full privileges.

  Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **High**

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0818
  Microsoft:
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms04-007.asp

- **15126 ISC BIND Negative Cache Poison Denial Of Service Vulnerability**

ISC BIND 8.3.x before 8.3.7, and 8.4.x before 8.4.3, allows remote attackers to poison the cache via a malicious name server that returns negative responses with a large TTL (time-to-live) value. To exploit this vulnerability, an attacker must configure a name server to return authoritative negative responses for a given target domain. Then, the attacker must convince a victim user to query the attacker's maliciously configured name server. When the attacker's name server receives the query, it will reply with an authoritative negative response containing a large TTL (time-to-live) value. If the victim's site runs a vulnerable version of BIND 8, it will cache the negative response and render the target domain unreachable until the TTL expires.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0914
CERT: http://www.kb.cert.org/vuls/id/734644
Security Focus: http://www.securityfocus.org/bid/9114/info/
Icat: http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0914

- **17872 ezContents 2.0.2 and prior 2.x PHP Code Injection Vulnerabilty**

ezContents a free open source content management system has been found to be vulnerable to Multiple PHP Code Injection vulnerabilities. They enable a malicious user to access arbitrary files or execute commands on the server.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0132
Web Site: http://www.ezcontents.org/forum/viewtopic.php?t=361

- **17873 phpgroupware 0.9.14.005 and prior PHP Code Injection Vulnerability**

phpGroupWare is a multi-user web-based groupware suite written in PHP. It also provides an API for developing additional applications. The product has been found to contain security vulnerabilities allowing a malicious user to view the true path under which the program has been installed and inject PHP code. Install the last phpgrougware stable version. Must be greater than 0.9.14.007.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: No CVE link available
phpgrougware Site: http://phpgroupware.org

- **17874 phpgroupware 0.9.14.005 and prior Multiple Vulnerabilities**

phpGroupWare is a multi-user web-based groupware suite written in PHP. The calendar module for phpgroupware 0.9.14 does not enforce the "save extension" feature for holiday files, which allows remote attackers to create and execute PHP files. Multiple

SQL injection vulnerabilities in the calendar and infolog modules for phpgroupware 0.9.14 allow remote attackers to perform unauthorized database operations.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0017
Debian: http://www.debian.org/security/2004/dsa-419

- **17876 ezContents 1.x PHP Code Injection Vulnerabilty**

ezContents a free open source content management system. PHP remote code injection vulnerability in module.php for ezContents allows remote attackers to execute arbitrary PHP code by modifying the link parameter to reference a URL on a remote web server that contains the code.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0070
Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107392588915627&w=2

New Vulnerabilities this Week

Arbitrary Remote Execution of Code in Microsoft Windows
Huge news. A vulnerability in Windows was announced this week can result in the remote execution of arbitrary code on the vulnerable system with System privileges. The vulnerability, which is a result of an unchecked buffer in the Microsoft ASN.1 Library, could lead to a buffer overflow. An attacker could then take any action on the system, including installing programs, viewing data, changing data, deleting data, and creating new accounts with full privileges. This patch has been in the works for a year. Microsoft wanted to get this one right. It is quickly being agreed that the *" Multiple Vulnerabilities in Microsoft ASN.1 Library "* may be one of the biggest security flaw ever found. SecureScout now has a Test Case for the patch.
For more information, see
http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/41750/WindowsSecurity_41750.html
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-007.asp
http://www.infoconomy.com/pages/news-and-gossip/group90711.adp
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/50341483?-2622
Source: Windows and .Net Magazine / Microsoft / Infoconomy / PC Advisor

phpCodeCabinet Input Validation Bugs Let Remote Users Conduct Cross-Site Scripting Attacks Some input validation vulnerabilities were reported in phpCodeCabinet. A remote user can conduct cross-site scripting attacks. It is reported that several scripts do not properly validate user-supplied input before displaying information based on the user input. A remote user can create a specially crafted request that, when executed by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the phpCodeCabinet software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any,

associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.
For more information, see http://securitytracker.com/alerts/2004/Feb/1009012.html
Source: SecurityTracker

Monkey httpd Denial of Service Vulnerability

Monkey is a Web server written in C that works under Linux. This is an open source project based on the HTTP/1.1 protocol. The objective is to develop a fast, efficient, small and easy to configure web server. The sending of some crafted HTTP requests leads to the freeze of the webserver. The problem is located in the function get_real_string().
For more information, see http://www.net-security.org/vuln.php?id=3253
http://monkeyd.sourceforge.net
Source: HelpNetSecurity

Internet Explorer and Microsoft Clipboard Poor Security Policy

In case you forgot, sensitive information can be unknowingly disclosed through use malicious web coding that exploits Internet Explorer and Microsoft clipboard. Recently, a brief test was run at a large corporation investigating means of execution and resulting security implications. Within this document you will find the code that was used for this research and a suggested solution. This is not a new problem. A similar hole in IE 5 was documented in March, 1999:
http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind9903&L=ntbugtraq&F=P&S=&P=6634
And again in January, 2002:
http://www.securityfocus.com/archive/1/250248/2004-02-07/2004-02-13/2 (links now broken)

Nearly five years later IE still by default Windows allows the clipboard to be made public. What's up with that? Well, at least they fixed the ASN.1 Library problem.
For more information, see http://www.securityfocus.com/archive/1/353508/2004-02-10/2004-02-16/0
Source: SecurityFocus

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. http://www.infosyssec.org/infosyssec/

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.