netVigilance

ScoutNews Team 20 February 2004

Issue #8

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Every week, some new virus or worm digs its way into our affections. This week it was NetSky.B and Bagel.B. When you update your SecureScout product this week, you will notice we now have Registry Checks for both these worms. I guess we've been hanging around the Linux box too much this week, as we have more Linux news and vulnerabilities than usual. And then there is the continuing story of the purloined Microsoft Win2000 and NT source code. Read what The Register has to say about the trustworthiness of MS Trustworthy Computing initiative.

Top Security News Stories this Week

❖ **Why Security Is No Longer IT's Ugly Stepsister**

First, it was Cisco's Super Bowl ad, in which a chief financial officer's daughter downloads a game that infects an entire network. Two weeks later--this time for real--Juniper acquired NetScreen Technologies for upward of $3 billion. These are the most visible examples, but if you listen to the strategies of other networking vendors like 3Com, Enterasys Networks, Extreme Networks or Nortel Networks, you can see the formation of a definite trend: Networking and security are moving closer together. While networking and security have been kissing cousins for years, a marriage looks more and more imminent. Why? First of all, both technologies monitor bits as they flow through the network. Networking equipment watches traffic to make routing, switching and quality-of-service decisions. Security devices eyeball the same traffic in search of protocol anomalies, known attack patterns, viruses and worms. Networking gear has had basic security functionality like packet filtering for years, but the thought of aggregating the two worlds wasn't really considered.

http://news.com.com/2010-7355_3-5161869.html?part=rss&tag=feed&subj=news
By Jon Oltsik - CNET

❖ **Serious Linux Security Holes Uncovered and Patched**

Several security vulnerabilities in the Linux kernel were uncovered this week by a Polish security group. The problems were verified by Linux kernel developers and then fixed with a set of updates. The Polish security non-profit organization iSEC Security Research released an advisory describing two "critical security vulnerabilities" in Linux 2.4 and 2.6's "kernel-memory-management code inside the "mremap(2)" system call. The first of the problems, called "Linux kernel do_mremap VMA limit local privilege escalation vulnerability" by iSEC, could have enabled a cracker to achieve full super-user privileges. With the super-user authority, equivalent to Windows' administrator mode, a malicious user could destroy other users' directories, plant rogue programs or trash the entire system. The second vulnerability, dubbed the "Linux kernel do_mremap() local privilege escalation vulnerability," could have with "proper exploitation of this vulnerability … lead to local privilege escalation including execution of arbitrary code with kernel-level access," the iSEC advisory explained. In short, an entire system could be disabled or hijacked.

http://www.eweek.com/article2/0,4149,1530811,00.asp?kc=EWRSS03119TX1K0000594
http://www.silicon.com/hardware/servers/0,39024647,39118519,00.htm
By Steven Vaughn – eWeek / Robert Lemos – Silicon.com

❖ NetSky.B and Bagle.B Worms Gain Traction

Did you catch this one? Alert IT pros nipped this one in the bud in most cases. On Tuesday and Wednesday a new mass-mailing worm, called NetSky.B, spread rapidly after beginning to make the rounds of e-mail inboxes. NetSky.B is a variant of the NetSky.A worm identified earlier in the week, but is posing a greater risk of spreading and infecting machines, security vendors warned Wednesday. Symantec Corp. rated NetSky.B a Category 4 threat, its second-highest level, while Network Associates Inc. and F-Secure Corp. rated it as a medium threat. NetSky.B is distributed through e-mails as a ZIP archive or an executable attachment. Computer experts said the infected e-mail comes with close to 50 different subject lines and body text, making it difficult to identify and stop. A similar virus labeled Bagle.B was also detected earlier this week. SecureScout now has Registry Checks for both of these.

http://www.eweek.com/article2/0,4149,1530599,00.asp?kc=EWRSS03119TX1K0000594
http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=5&u=/afp/20040219/tc_afp/internet_virus&sid=96001018
http://www.itweb.co.za/sections/techforum/2004/0402190836.asp?O=FPMP
By Matt Hicks – eWeek / Yahoo News / Zea Silva -ITWeb

❖ Microsoft Borrows From RIAA's Playbook

Anxious to stop the spread of its purloined Windows source code, Microsoft is sending letters to computer users who are downloading the intellectual property, requesting they stop. It is a move reminiscent of the music industry's early tactics to stem the sharing of copyrighted material on peer-to-peer networks. However, the similarity may end there, as Microsoft says it is not threatening to sue downloaders - yet. "It is illegal for third parties to post Microsoft source code, and we take such activity very seriously," the company said. As we reported last week, a portion of Microsoft's Windows 2000 and NT source code -- arguably the software titan's most valuable trade secret -- leaked onto the Internet. It is now circulating on several P2P networks. Microsoft is working with law-enforcement authorities to investigate the postings.

http://www.newsfactor.com/story.xhtml?story_title=Microsoft_Borrows_from_RIAA_s_Playbook&story_id=23209&category=netsecurity
http://www.infosyssec.com/cgibin/flink.cgi?target=www.infosyssec.com/infosyssec/ab11.htm
By Erika Morphy – Newsfactor.com / Steve Ranger - vnunet

- **Microsoft's Shared-Source Defeats Trustworthy Computing**

  The recent leak of Windows source code onto the Web has made a lot of people jumpy. According to MS news blog Bink.nu, the company has already discovered at least one downloader and sent him a nastygram. If this is true, it indicates an aggressive response back in Redmond, a scrambling to plug the leaks and intimidate in the curious RIAA-style. It should surprise no one that the proverbial chickens have come home to roost. Microsoft's security is in part a function of keeping its source code out of the wrong hands. Thus the Shared Source gimmick is in direct conflict with that portion of the company's Trustworthy Computing gimmick that depends on secrecy. No one wants malicious coders to get their hands on enough of the Windows source to accelerate development of the never-ending torrent of novel exploits already coming out on a weekly basis.

  http://www.theregister.co.uk/content/55/35659.html
  By Thomas Green - The Register UK

New Vulnerabilities Tested in SecureScout

Eight new vulnerability Test Cases have been incorporated into the SecureScout database this week including a Registry Check for the NetSky.B and Bagel.B worms! Of course, these weekly updates are what keeps your network scanning tool one step in front of the hackers, inside or outside the organization.

- **12103 Oracle9i Database Multiple Buffer Overflow Vulnerabilities**

  Multiple vulnerabilities in Oracle9i Database have been reported, which can be exploited by malicious database users to compromise the system and gain escalated privileges.

  The first vulnerabilities are caused due to boundary errors in two functions used for interval conversion ("NUMTOYMINTERVAL" and "NUMTODSINTERVAL"). These can be exploited to cause buffer overflows by supplying an overly long "char_expr" string.

  These two vulnerabilities have been reported in versions prior to 9.2.0.4 (Patchset 3).

  The last two vulnerabilities are caused due to boundary errors in the "FROM_TZ" function and in the "TIME_ZONE" parameter.

  Both vulnerabilities reportedly affect versions prior to 9.2.0.3.

  Successful exploitation of the vulnerabilities may allow a malicious, unprivileged database user to execute arbitrary code with either SYSTEM or ORACLE privileges.

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

  CVE Link: No CVE link available
  Product Homepage: http://www.oracle.com/
  NGSSoftware:
  Oracle NUMTOYMINTERVAL Remote System Overflow
  http://www.nextgenss.com/advisories/ora_numtoyminterval.txt
  Oracle NUMTODSINTERVAL Remote System Overflow
  http://www.nextgenss.com/advisories/ora_numtodsinterval.txt

Oracle TIME_ZONE Remote System Buffer Overrun
http://www.nextgenss.com/advisories/ora_time_zone.txt
Oracle FROM_TZ Remote System Buffer Overrun
http://www.nextgenss.com/advisories/ora_from_tz.txt

- **14400 RealPlayer & RealOne Player Buffer Overruns**

The remote host has RealPlayer installed. There is a flaw in the remote version which may allow an attacker to execute arbitrary code on the remote host, with the privileges of the user running RealPlayer. To do so, an attacker would need to send a corrupted RMP file to a remote user and have him open it using RealPlayer.

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

CVE Link: No CVE link available
Security Focus: http://securityfocus.com/archive/1/352780
http://securityfocus.com/bid/9580
CVSWeb: http://cvsweb.nessus.org/cgi-bin/cvsweb.cgi/~checkout~/nessus-plugins/scripts/realplayer_file_handler_overflow.nasl?content-type=text/plain

- **14402 LanMan Authentication**

LanMan authentication is poor. Passwords sent using that method can be easily discovered. You would rather prefer to use NTLM, or if feasible, only NTLMv2. To fix the vulnerability you must update your registry configuration and change the "LMCompatibilityLevel" DWORD value to 3 within the following registry location: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

Note that the change will break functionality with legacy systems as Windows 95/98.

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

CVE Link: No CVE link available
eEye: http://www.eeye.com/html/Products/Retina/RTHs/Registry/182.html
Microsoft:
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q147/7/06.asp&NoWebContent=1
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/protech/win2000/win2khg/05sconfg.asp

- **14404 Remote Access Server Logging**

MS Remote Access Server is not logging connections. It is recommended to log all RAS connection information.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Medium**

CVE Link: No CVE link available
eEye: http://www.eeye.com/html/Products/Retina/RTHs/Registry/209.html

Packet Storm: http://packetstormsecurity.nl/NT/Release-RegFix.reg.TXT
Microsoft: http://support.microsoft.com/default.aspx?scid=kb;%5BLN%5D;234014
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0502.asp

- **14405 MSCHAPv2 Authentication for VPN**

MSCHAP V2 is a more secure protocol for VPN authentication. It is recommended to force the server to drop any VPN (Virtual Private Network) connections that do not use MSCHAP V2 authentication. It is recommended that you only enable MSCHAPv2 for VPN authentication by adding the following DWORD "SecureVPN" with a value of 1 under the following registry location:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\PPP

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

CVE Link: No CVE link available
eEye: http://www.eeye.com/html/Products/Retina/RTHs/Registry/185.html

- **14406 Scheduler Service Started**

If you do not use the Task scheduler you should disable the service. The task scheduler is often used in malicious hacking attacks to run Trojan code. It has also been used in the past to elevate local privileges. It is recommended that you disable the Task scheduler service by updating the the following DWORD "Start" with a value of 4 under the following registry location:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Medium**

CVE Link: No CVE link available
eEye: http://www.eeye.com/html/Products/Retina/RTHs/Registry/899.html

- **14407 W32/Bagle.b Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:

- Contains its own SMTP engine to construct outgoing messages
- Harvests email addresses from the victim machine the From: address of messages is spoofed
- Contains a remote access component (notification is sent to hacker)

This worm checks the system date. If it is the 25th February 2004 or later, the worm simply exits and does not propagate.

If the date check is satisfied, the virus executes the standard Windows Sound Recorder (SNDREC32.EXE) application.

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

CVE Link: No CVE link available
McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101030

- **14408 W32/Netsky.b Worm (Registry Check)**

  This virus spreads via email and mapped drives. It sends itself to addresses found on the victim's machine and by copying itself to folders on drives C: & Z: The virus also attempts to deactivate the W32/Mydoom.a@MM and W32/Mydoom.b@MM viruses.

  The virus sends itself via SMTP - constructing messages using its own SMTP engine. It queries the DNS server for the MX record and connects directly to the MTA of the targeted domain and sends the message. When executed, a fake error message may be displayed.

  The worm copies itself to directories named share or sharing on the local system and on mapped network drives. This will result in propagation via KaZaa, Bearshare, Limewire, and other P2P application that use shared folder names containing the words share or sharing. The filenames are included in the worm and chosen randomly.

  The worm also drops numerous ZIP files containing the worm (22,016 bytes). The compressed file frequently uses a double extension like .doc.pif, .rtf.com, .rtf.scr). The list of ZIP names is hard coded in the virus body.

  The virus removes some registry values to deactivate Mydoom.a and Mydoom.b.

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

  CVE Link: No CVE link available
  McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101034

New Vulnerabilities this Week

Cisco ONS Devices Grant Remote Users Access Via TFTP and Can Also Be Reset
It is reported that a remote user can connect to the TFTP service on UDP port 69 and execute GET and PUT commands. A remote user can reportedly retrieve ONS system files on the active TCC in the /flash0 or /flash1 directories. A remote user can cause denial of service conditions by uploading corrupt ONS system files to the controller card, the report said.

It is also reported that a remote user can connect to TCP port 1080 and fail to send the final ACK handshake to cause denial of service on the Cisco ONS 15327, ONS 15454, and ONS 15454 SDH devices. This will cause the controller card to reset. On the Cisco ONS 15454, ONS 15327, and ONS 15454 SDH hardware, traffic will be temporarily dropped from the synchronous data channels while both the active and standby control cards are rebooting. Cisco has assigned bug ID CSCec17406 to this vulnerability.

It is also reported that a remote user can connect to the telnet port and access a superuser account that has been locked out, disabled, or suspended by using the previously configured password for the account. Cisco has assigned bug ID CSCec66884 to this issue on the Cisco ONS 15327, ONS 15454 and ONS 15454 SDH, and Cisco bug ID CSCec71157 to this issue on the Cisco ONS

15600 hardware. The impact:

- A remote user can access the system via TFTP to view certain files and potentially upload malformed system files.
- A remote user with previously valid authentication credentials can access the system.
- A remote user can cause the controller card to reset. In certain cases, network traffic may be affected

For more information, see http://www.securitytracker.com/alerts/2004/Feb/1009137.html
Source: Security Tracker

SUSE Linux Kernel Security Alert

Another bug in the Kernel's do_mremap() function, which is unrelated to the bug fixed in SuSE-SA:2004:001, was posted this week. The do_mremap() function of the Linux Kernel is used to manage Virtual Memory Areas (VMAs) which includes moving, removing and resizing of memory areas. To remove old memory areas do_mremap() uses the function du_munmap() without checking the return value. By forcing do_munmap() to return an error the memory management of a process can be tricked into moving page table entries from one VMA to another. The destination VMA may be protected by a different ACL which enables a local attacker to gain write access to previous read-only pages. The result will be local root access to the system. Check here to see if your OS is affected and for a list of CVE links.
For more information, see http://www.securityfocus.com/advisories/6349
Source: SecurityFocus

OpenLinux: Bind: cache poisoning BIND 8 prior to 8.3.7 and BIND 8.4.x prior 8.4.2

We’re on a Linux kick this week. As you know, BIND is an implementation of the Domain Name System (DNS) protocols. Successful exploitation of this vulnerability may result in a temporary denial of service. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2003-0914 to this issue.
For more information, see http://www.securityfocus.com/advisories/6358
Source: Security Focus
ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/Server/CSSA-2004-003.0/RPMS
ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/Server/CSSA-2004-003.0/SRPMS

Coreutils LS Width Argument Integer Overflow Vulnerability

Coreutils 'ls' has been reported prone to an integer overflow vulnerability. The issue reportedly presents itself when handling width and column display command line arguments. It has been reported that excessive values passed as a width argument to 'ls' may cause an internal integer value to be misrepresented. Further arithmetic performed based off this misrepresented value may have unintentional results. Additionally it has been reported that this vulnerability may be exploited in software that implements and invokes the vulnerable 'ls' utility to trigger a denial of service in the affected software.
For more information, see http://www.securityfocus.com/bid/8875/info/
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.