ScoutNews Team **17 December 2004**
Issue #51

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

There is absolutely no slowdown in new vulnerabilities that surface or get exploited.
This week a hacker was sentenced to 9 (nine) years in jail.
Microsoft will offer a beta version of a spyware remover, but will try to have end users pay for this service in the future. AND… big is beautiful say Symantec, Oracle, Microsoft etc. as well as analysts; however end users don't seem to agree that this goes for everything.

At netVigilance we believe you still need the independent and unbiased security companies like ourselves to police the bigger and more integrated suppliers.
Be sure to contact your netVigilance representative if you have more needs or budget dollars that need to be spent on security before the end of the year.

Enjoy reading

Top Security News Stories this Week

Wi-Fi Hacker Sentenced To Nine Years
A 21-year-old Michigan man was sentenced Wednesday to nine years in prison for breaking into the network of home improvement retailer Lowe's, the longest jail term ever handed out in the U.S. for hacking.
Brian Salcedo pleaded guilty in August to various charges, including conspiracy and fraud, stemming from a 2003 incident in which he and two others were caught hacking into an unsecured Wi-Fi access point from the parking lot of a Lowe's in suburban Detroit. They then accessed Lowe's national computer system -- which is based in North Wilkesboro, N.C. -- and installed a program to hijack credit card information.
http://story.news.yahoo.com/news?tmpl=story&ncid=1293&e=8&u=/cmp/20041217/tc_cmp/

55800486&sid=95573432
Tech Web

Microsoft Software to Remove Spyware
Microsoft Corp. disclosed plans Thursday to offer frustrated users of its Windows software new tools within 30 days to remove spyware programs secretly running on computers. But it might cost extra in coming months.
In a shift from past practice, the world's largest software manufacturer said it may charge consumers for future versions of the new protective technology, which Microsoft acquired by buying a small New York software firm. Terms of the sale of Giant Company Software Inc. weren't disclosed.
http://story.news.yahoo.com/news?tmpl=story&ncid=1209&e=1&u=/ap/20041218/ap_on_hi_te/microsoft_spyware&sid=95573712
Ted Bridis

Analysis: PeopleSoft users speak out about Oracle takeover
The great debate over the impact of Oracle's hostile takeover of PeopleSoft has all the big industry analyst organizations weighing in. However, in most of the analysis one group's opinion seems to have been overlooked: that of PeopleSoft users.
What follows is a sampling of recent PeopleSoft user comments, e-mailed to *InfoWorld*, on many of the issues surrounding Oracle's hostile takeover.
Most of the users asked *InfoWorld* not to publish their name or company. In that spirit, the editors have deleted all references in case a letter writer regrets it later.
http://story.news.yahoo.com/news?tmpl=story&ncid=1208&e=1&u=/infoworld/20041218/tc_infoworld/51941&sid=96742471
Ephraim Schwartz

New Vulnerabilities Tested in SecureScout

14159 Samba Security Descriptor Parsing Integer Overflow Vulnerability
Samba is an application designed to facilitate integrated file sharing between Unix/linux based machines and Windows machines. Samba uses Windows based protocols and share methods to facilitate this.

Remote exploitation of an integer overflow vulnerability in all versions of Samba's smbd prior to and including 3.0.8 could allow an attacker to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges.

To open a file on a Samba server, a client sends a sequence of SMB messages to the smbd process. The message with the information on the file to open also contains a security descriptor, which is a list of access controls to apply to the file. The vulnerability specifically occurs in the allocation of memory to store these descriptors.

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

CVE Links: CAN-2004-1154

Reference: http://us1.samba.org/samba/security/CAN-2004-1154.html & http://www.idefense.com/applicat...?id=165&type=vulnerabilities

15135 Vulnerability in WordPad Could Allow Code Execution (MS04-041/885836) (Remote File Checking)

A remote code execution vulnerability exists in the Microsoft Word for Windows 6.0 Converter. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system. However, user interaction is required to exploit this vulnerability.

A remote code execution vulnerability exists in the Microsoft Word for Windows 6.0 Converter. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system. However, user interaction is required to exploit this vulnerability.

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

CVE Links: CAN-2004-0571 & CAN-2004-0901

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-041.mspx

15136 Vulnerability in DHCP Could Allow Remote Code Execution and Denial of Service (MS04-042/885249) (Remote File Checking)

A denial of service vulnerability exists that could allow an attacker to send a specially crafted DHCP message to a DHCP server. An attacker could cause the DHCP Server service to stop responding.

A remote code execution vulnerability exists that could allow an attacker to send a specially crafted DHCP message to a DHCP server. However, attempts to exploit this vulnerability would most likely result in a denial of service of the DHCP Server service.

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

CVE Links: CAN-2004-0899 & CAN-2004-0900

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-042.mspx

15137 Vulnerability in HyperTerminal Could Allow Code Execution (MS04-043/873339) (Remote File Checking)

A remote code execution vulnerability exists in HyperTerminal because of a buffer overrun. An attacker could exploit the vulnerability by constructing a malicious HyperTerminal session file that could potentially allow remote code execution. An attacker could then persuade a user to open this file. This vulnerability could attempt to be exploited through a malicious Telnet URL if HyperTerminal has been set as the default Telnet client. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability

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

CVE Link: CAN-2004-0568

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-043.mspx

15138 Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (MS04-044/885835) (Remote File Checking)

A privilege elevation vulnerability exists in the way that the Windows Kernel launches applications. This vulnerability could allow a logged on user to take complete control of the system.

A privilege elevation vulnerability exists in the way that the LSASS validates identity tokens. This vulnerability could allow a logged on user to take complete control of the system.

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

CVE Link: CAN-2004-0893 & CAN-2004-0894

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-044.mspx

15139 Vulnerability in WINS Could Allow Remote Code Execution (MS04-045/870763) (Remote File Checking)

A remote code execution vulnerability exists in WINS because of the way that it handles computer name validation. An attacker could exploit the vulnerability by constructing a malicious network packet that could potentially allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in WINS because of the way that it handles association context validation. An attacker could exploit the vulnerability by constructing a malicious network packet that could potentially allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, attempts to exploit this vulnerability would most likely result in a denial of service on Windows Server 2003. The service would have to be restarted to restore functionality.

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

CVE Link: CAN-2004-0567 & CAN-2004-1080

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-045.ms

15141 Ethereal DICOM dissector (Remote File Checking)

Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An unspecified error within the DICOM dissector can be exploited to crash Ethereal.

The vulnerability affects versions 0.10.4 through 0.10.7.

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

CVE Link: CAN-2004-1139

Reference: http://www.ethereal.com/appnotes/enpa-sa-00016.html#details

15142 Ethereal invalid RTP timestamp (Remote File Checking)
Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An unspecified error within the handling of RTP timestamps can be exploited to cause Ethereal to stop responding and create a large temporary file, which may consume all available disk space.

The vulnerability affects versions 0.9.16 through 0.10.7.

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

CVE Link: CAN-2004-1140

Reference: http://www.ethereal.com/appnotes/enpa-sa-00016.html#details

15143 Ethereal HTTP dissector accessing previously-freed memory (Remote File Checking)
Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An unspecified error within the HTTP dissector may result in freed memory being accessed, which causes Ethereal to crash.

The vulnerability affects versions 0.10.1 through 0.10.7.

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

CVE Link: CAN-2004-1141

Reference: http://www.ethereal.com/appnotes/enpa-sa-00016.html#details

15144 Ethereal improperly formatted SMB packet (Remote File Checking)
Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An unspecified error within the SMB dissector can be exploited via a specially crafted SMB packet to cause Ethereal to stop responding and consume a large amount of CPU resources.

The vulnerability affects versions 0.9.0 through 0.10.7.

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

CVE Link: CAN-2004-1142

Reference: http://www.ethereal.com/appnotes/enpa-sa-00016.html#details

New Vulnerabilities found this Week

Veritas Backup Exec Registration Request Buffer Overflow
"Execution of arbitrary code"
A vulnerability has been reported in VERITAS Backup Exec, which can be exploited by malicious people to compromise a vulnerable system.
The vulnerability is caused due to a boundary error in the Agent Browser service when processing received registration requests and can be exploited to cause a stack-based buffer overflow.
Successful exploitation allows execution of arbitrary code.
References:
http://seer.support.veritas.com/docs/273419.htm

Vim / Gvim Modelines Command Execution Vulnerabilities
"Gain escalated privileges"
Ciaran McCreesh has reported some vulnerabilities in vim and gvim, which can be exploited by malicious, local users to gain escalated privileges.
The vulnerabilities are caused due to some errors in the modelines options. This can be exploited to execute shell commands when a malicious file is opened.
Successful exploitation can lead to escalated privileges but requires that modelines is enabled.
References:
http://www.gentoo.org/security/en/glsa/glsa-200412-10.xml

Cisco Guard Inappropriate Default "root" Password
"Gain access to the administrative account"
A weakness has been reported in Cisco Guard, which potentially allows malicious people to gain access to the administrative account.
The problem is that Cisco Guard inappropriately sets a default password for the "root" account during installation instead of prompting the user for a new password.
Successful exploitation will provide access to the system.
This affects all Cisco Guard versions prior to 3.1.
References:
http://www.cisco.com/en/US/produ...y_advisory09186a008037d0c5.shtml

Cisco Unity Default Usernames and Passwords
"Access administrative functions"
A security issue has been reported in Cisco Unity, which can be exploited by malicious

people to access administrative functions.
The problem is that Cisco Unity creates certain user accounts with default passwords when integrated with Exchange.
Successful exploitation provides access to certain administrative functions.
The issue affects Cisco Unity versions 2.x, 3.x, and 4.x (prior to version "4.0(5)") when integrated with Exchange. Cisco Unity integrated with Lotus Notes is not affected.
References:
http://www.cisco.com/warp/public/707/cisco-sa-20041215-unity.shtml

Samba Security Descriptor Parsing Integer Overflow Vulnerability
“Execution of arbitrary code”
iDEFENSE has reported a vulnerability in Samba, which can be exploited by malicious users to compromise a vulnerable system.
The vulnerability is caused due to an integer overflow within smbd when handling security descriptors. This can be exploited to cause a heap-based buffer overflow by requesting an extremely large amount of security descriptors.
Successful exploitation allows execution of arbitrary code, but requires that the user has proper credentials to access a share.
The vulnerability affects versions 2.x and 3.0.x up to and including version 3.0.9.
References:
http://us1.samba.org/samba/security/CAN-2004-1154.html

Adobe Acrobat Reader "mailListIsPdf()" Function Buffer Overflow
“Execution of arbitrary code”
iDEFENSE has reported a vulnerability in Adobe Acrobat Reader, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error in the "mailListIsPdf()" function when checking input files. This can be exploited to cause a buffer overflow by e.g. sending an e-mail with a malicious PDF document attached or a link to one.
Successful exploitation allows execution of arbitrary code.
The vulnerability has been reported in version 5.0.9 for Unix. Prior versions may also be affected.
References:
http://www.adobe.com/support/techdocs/331153.html

Adobe Reader / Adobe Acrobat Multiple Vulnerabilities
“Execute arbitrary code”
Some vulnerabilities have been reported in Adobe Reader and Adobe Acrobat, which can be exploited by malicious people to disclose sensitive information or compromise a user's system.
1) A format string error within the eBook plug-in when parsing ".etd" files can be exploited to execute arbitrary code via a specially crafted eBook containing format specifiers in the "title" and "baseurl" fields.
2) Multiple vulnerabilities in libpng have been acknowledged, which can be exploited by malicious people to compromise a vulnerable system.
3) An error within the handling of Flash files embedded in PDF documents can be exploited to read the content of files on a user's system.

The vulnerabilities have been reported in versions 6.0.0 through 6.0.2.
References:
http://www.adobe.com/support/downloads/detail.jsp?ftpID=2679

Linux Kernel IGMP and "__scm_send()" Vulnerabilities
"Denial of Service"
Paul Starzetz has reported some vulnerabilities in the Linux Kernel, which can be exploited by malicious people to cause a DoS (Denial of Service), and by malicious, local users to cause a DoS, gain knowledge of sensitive information, or potentially gain escalated privileges.
1) An error in the "ip_mc_source()" function of the IGMP (Internet Group Management Protocol) subsystem can be exploited by malicious, local users to overwrite kernel memory, which crashes the system and may allow users to gain escalated privileges. This vulnerability can also be further exploited via the "ip_mc_msfget()" and "ip_mc_gsfget()" user API functions to disclose large portions of kernel memory.
2) The "igmp_marksources()" function of the IGMP networking module does not validate received IGMP message parameters properly, which may result in an out-of-bounds memory access error. This can be exploited by malicious people to cause a vulnerable system to hang or potentially crash via specially crafted IGMP_HOST_MEMBERSHIP_QUERY messages.
Successful exploitation requires that the kernel is compiled with multicasting support and is processing incoming IGMP packets. It is further required that an application has a bound multicast socket with attached source filter.
3) A deadlock condition in the "__scm_send()" scm message parsing function can be exploited by malicious, local users to cause the system to hang via a specially crafted auxiliary message sent to a socket.
The vulnerabilities have been reported in versions 2.4 through 2.4.28 and 2.6 through 2.6.9.
References:
http://isec.pl/vulnerabilities/isec-0018-igmp.txt
http://isec.pl/vulnerabilities/isec-0019-scm.txt

Ethereal Multiple Vulnerabilities
"Denial of Service"
Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.
1) An unspecified error within the DICOM dissector can be exploited to crash Ethereal.
The vulnerability affects versions 0.10.4 through 0.10.7.
2) An unspecified error within the handling of RTP timestamps can be exploited to cause Ethereal to stop responding and create a large temporary file, which may consume all available disk space.
The vulnerability affects versions 0.9.16 through 0.10.7.
3) An unspecified error within the HTTP dissector may result in freed memory being accessed, which causes Ethereal to crash.
The vulnerability affects versions 0.10.1 through 0.10.7.
4) An unspecified error within the SMB dissector can be exploited via a specially crafted SMB packet to cause Ethereal to stop responding and consume a large amount of CPU

resources.
The vulnerability affects versions 0.9.0 through 0.10.7.
References:
http://www.ethereal.com/appnotes/enpa-sa-00016.html

phpMyAdmin Two Vulnerabilities
"Disclose sensitive information"
Nicolas Gregoire has reported two vulnerabilities in phpMyAdmin, which can be exploited by malicious people to compromise a vulnerable system and by malicious users to disclose sensitive information.
1) An input validation error in the handling of MySQL data allows injection of arbitrary shell commands.
Example:
F\';[command]\'A
Successful exploitation requires that PHP safe mode is disabled and MIME-based external transformations are activated.
The vulnerability has been reported in versions 2.6.0-pl2 up to 2.6.1-rc1.
2) Input passed to "sql_localfile" is not properly sanitised in "read_dump.php" before being used to disclose files.
Successful exploitation requires access to the phpMyAdmin interface, and that PHP safe mode is disabled and the UploadDir mechanism to be active.
The vulnerability has been reported in versions 2.4.0 up to 2.6.1-rc1.
References:
http://www.exaprobe.com/labs/advisories/esa-2004-1213.html
http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2004-4

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.

About SecureScout
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net