netVigilance

ScoutNews Team **20 November 2004**
Issue #47

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The Sober worm is just one in a long chain of worms that are on their war to make 2004 the year of worms.
One more trend is starting that may dominate in 2005; Worms and Viruses that target cell phones.

Enjoy reading

Top Security News Stories this Week

- **Fast-Spreading Sober Worm Up In Europe, Heading To U.S.**

A new Sober worm began spreading early Friday morning in Europe and quickly gained enough traction worldwide that security companies scrambled to warn users and produce new signatures to deflect the attack.
Sober.i is the general designation by anti-virus firms, although McAfee dubbed it Sober.j. By mid-morning, virtually every security vendor had popped its warning level to "medium," although Panda Software tagged it with a "high" label.
http://www.crn.com/sections/breakingnews/dailyarchives.jhtml%3Bjsessionid=TIVD51T2G50H2QSNDBGCKH0CJUMEKJVN?articleId=53700907
Gregg Keizer

- **New virus detected for phones running Series 60**

F-Secure Corp. said it discovered a new Trojan computer virus for mobile phones running the Series 60 version of the Symbian operating system. The company said the bug replaces menu icons on the phone with a skull-and-crossbones symbol, and locks up the phone and prevents it from booting up.
http://rcrnews.com/news.cms?newsId=20512
Mike Dano

New Vulnerabilities Tested in SecureScout

- **13178 Skype "callto:" URI Handler Buffer Overflow Vulnerability (Remote File Checking)**

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology

to bring affordable and high-quality voice communications to people all over the world.
Vulnerability has been reported which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error within the handling of command line arguments. This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into visiting a malicious web site, which passes an overly long string (more than 4096 bytes) to the "callto:" URI handler.
Successful exploitation may allow execution of arbitrary code.
The vulnerability affects versions 1.0.*.95 through 1.0.*.98.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.skype.com/ & http://www.skype.com/products/skype/windows/ & http://secunia.com/advisories/13191/

- **14045 Samba QFILEPATHINFO Request Handler Buffer 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.
During an audit of the Samba 3.x codebase a unicode filename buffer overflow within the handling of TRANSACT2_QFILEPATHINFO replies was discovered that allows remote execution of arbitrary code.
Exploiting this vulnerability is possible through every Samba user if a special crafted pathname exists. If such a path does not exist the attacker needs write access to one of the network shares.

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

CVE Links: CAN-2004-0882

Reference: http://security.e-matters.de/advisories/132004.html & http://www.samba.org

- **14046 Samba Wildcard Filename Matching Denial of Service 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 input validation error in Samba could allow an attacker to consume system resources and potentially cause the target system to crash.
Successful exploitation allows authenticated remote attackers to exhaust CPU resources. This attack takes very little bandwidth and can, in some cases, cause the machine to stop responding. Multiple attacks can be
launched in parallel which can make this attack more effective.

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

CVE Links: CAN-2004-0930

Reference: http://www.samba.org &

http://www.idefense.com/application/poi/display?id=156&type=vulnerabilities&flashstatus=true

- **14047 Samba Arbitrary File Access 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 input validation vulnerability in Samba allows attackers to access files and directories outside of the specified share
  path.
  Successful exploitation allows remote attackers to bypass the specified share restrictions to gain read, write and list access to files and directories under the privileges of the user. In situations where a public share is available, the attack can be performed by unauthenticated attackers.
  An attacker does not need exploit code to exploit this vulnerability. The smbclient program can be used to request/write/list files using the "get", "put" and "dir" commands, respectively.

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

CVE Link: CAN-2004-0815

Reference: http://www.samba.org &
http://www.idefense.com/application/poi/display?id=146&type=vulnerabilities

- **15565 SMTP server fakes Postfix in HELP answer**
  Postfix is a commonly used SMTP server for unix platforms. This server does not respond to HELP commands.

Test Case Impact: **Gather info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.postfix.com/

- **15566 Fake Sendmail Version in Banner**
  Sendmail is a commonly used SMTP server for unix platforms. This Sendmail server shows a fake version in the banner.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.sendmail.org/

- **15567 Fake Sendmail Version in HELP command answer**
  Sendmail is a commonly used SMTP server for unix platforms. This Sendmail server shows a fake version in the HELP command answer.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.sendmail.org/

- **17927 phpMyAdmin Input Validation Errors in 'read_dump.php' XSS Vulnerability**

  phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW.
  When performing a request to 'read_dump.php', a variable called 'zero_rows' can be used to display a specific message when the result from the MySQL server doesn't contain any row. This variable is not well sanatized, permitting to conduct XSS attack in case of 0 row answer from the Database.
  This 0 row answer, can be triggered by a request like 'set @1=1'.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.netvigilance.com/html/advisory0005.htm & http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2004-3 & http://www.phpmyadmin.net/home_page/

- **17928 phpMyAdmin URL Validation Errors in 'config.inc.php' XSS Vulnerability**

  phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW.
  If the configuration parameter $cfg['PmaAbsoluteUri'] is not set in the config.inc.php file, the auto-detect process can be used to conduct XSS attacks, using the following URL pattern
  'HTTP://[target]/[phpMyAdmin_directory]/[file]?[parameters1]/[parameters2]'

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.netvigilance.com/html/advisory0005.htm & http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2004-3 & http://www.phpmyadmin.net/home_page/

- **17929 phpMyAdmin Input Validation Erros in 'Confirm form' XSS Vulnerability**

  phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW.
  For some specific SQL statements a confirm page may be needed.
  This confirm page (generated by sql.php) will embed a form which can be used to conduct XSS attack.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.netvigilance.com/html/advisory0005.htm & http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2004-3 & http://www.phpmyadmin.net/home_page/

New Vulnerabilities found this Week

- **Linux Kernel smb Filesystem Implementation Multiple Vulnerabilities**

"Denial of Service"

Stefan Esser has reported multiple vulnerabilities in the Linux kernel, which can be exploited by malicious people to cause a DoS (Denial of Service) or leak kernel memory. Reportedly, it is currently unclear whether some of the vulnerabilities also can be exploited for arbitrary code execution.

The vulnerabilities are located within the smb filesystem (smbfs) implementation and are caused due to various types of errors when handling server responses.

Successful exploitation requires that a malicious person has control over a smb server or is able to intercept and manipulate traffic.

NOTE: Not all vulnerabilities affect both the 2.4 and 2.6 kernels (see the original advisory for more information).

References:

http://security.e-matters.de/advisories/142004.html

- **X11 libXpm Multiple Image Processing Vulnerabilities**

"Denial of Service"

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

The vulnerabilities are caused due to various types of errors including integer overflows, out-of-bounds memory access, and input validation errors. These can be exploited by tricking a user into viewing a specially crafted image in an application linked against the vulnerable library.

The vulnerabilities have been reported in version 6.8.1 and prior.

References:

http://www.x.org/pub/X11R6.8.1/patches/README.xorg-681-CAN-2004-0914.patch

- **Microsoft Internet Explorer Cookie Path Attribute Vulnerability**

"Session fixation attacks"

Keigo Yamazaki has reported a vulnerability in Internet Explorer, which potentially can be exploited by malicious people to conduct session fixation attacks.

The vulnerability is caused due to a validation error in the handling of the path attribute when accepting cookies. This can potentially be exploited by a malicious website, if the trusted site supports wildcard domains or the domain name contains the malicious sites domain, using a specially crafted path attribute to overwrite cookies for the trusted site.

The vulnerability has been reported in Internet Explorer 6.0 SP1 on Microsoft Windows XP SP1. Microsoft Windows XP SP2 is reportedly not affected.

Note: Successful exploitation also requires that the trusted site handles cookies and

authentication in an inappropriate or insecure manner.
References:
http://www.lac.co.jp/business/sns/intelligence/SNSadvisory_e/79_e.html

- **Skype "callto:" URI Handler Buffer Overflow Vulnerability**

"Execution of arbitrary code"

A vulnerability has been reported in Skype, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error within the handling of command line arguments. This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into visiting a malicious web site, which passes an overly long string (more than 4096 bytes) to the "callto:" URI handler.
Successful exploitation may allow execution of arbitrary code.
The vulnerability affects versions 1.0.*.95 through 1.0.*.98.
References:
http://www.skype.com/products/skype/windows/

- **Samba QFILEPATHINFO Request Handler Buffer Overflow Vulnerability**

"Execution of arbitrary code"

Stefan Esser has reported a vulnerability in Samba, which can be exploited by malicious users to compromise a vulnerable system.
The vulnerability is caused due to a boundary error in the QFILEPATHINFO request handler when constructing "TRANSACT2_QFILEPATHINFO" responses and can be exploited to cause a buffer overflow.
Successful exploitation allows execution of arbitrary code, but requires that a special pathname exists or that the user has write permissions on a network share.
The vulnerability has been reported in version 3.0.7 and prior.
References:
http://security.e-matters.de/advisories/132004.html
http://www.kb.cert.org/vuls/id/457622

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