netVigilance

ScoutNews Team **September 2, 2005**
Issue # 35

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

IE vulnerability exposes users to noxious pop-ups, Windows worm hits MP3 players and Spammers / Phishers still increasingly successful.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Symantec vulnerability exposes users to**

A vulnerability in Symantec's Anti Virus Corporate Edition Version 9 could allow an attacker or nonprivileged user to obtain sensitive server log-in information. The flaw affects organizations that have deployed an internal LiveUpdate server, which distributes anti-virus definition updates to Symantec software clients on a corporate network.

Symantec Corporate Anti-Virus stores Information about each update that includes the username and password used to access the server in unencrypted logs.
eWEEK

Full Story:
http://news.yahoo.com/news?tmpl=story&u=/zd/20050902/tc_zd/159414

❖ IE flaws exposes users to key logging pop-ups.

Sunbelt Software has reported a pop-up that takes advantage of an IE vulnerability in that lets it download the keystroke-logging application on a user's PC as soon as the user goes to a website at targeted banks. Although most banks use browser encryption, the malicious pop-up can capture data before it is encrypted. And because the exploit is new, current antivirus software can't block it.

CMP Security Pipeline

Full Story :
http://www.securitypipeline.com/news/170102451

❖ Windows worm infects Creative MP3 players.

Creative has issued a recall on some 4,000 Zeon Neon MP3 music players because of a Windows worm riding inside. There is little likelihood that the Wullik.b worm within the MP3 players could infect an attached PC, but the possibility does exist. If you have up to date virus protection and patches; you should be safe.

NewsFactor Technology News

Related Links:
http://www.newsfactor.com/news/Creative-Recalls-Infected-MP3-Players/story.xhtml?story_id=00100015P5PU

❖ Despite growing awareness, Spammers still are stealing from internet users

Numbers continue to grow for the prevalence and cost of these Phishing scams. The well-publicized Nigerian email fraud scheme that promises large sums of money to receipients that help move money from Nigeria to the US was $2,649 while auction scams resulted in an average loss of $765 and general merchandise of $846.

The Nigerian scam was the third-largest reported menace affecting users in 2004, at 9 percent. It followed auction (51 percent) and general merchandise (20 percent) scams that promise, but don't deliver, goods.

Source

Related Links:
http://www.internetnews.com/xSP/article.php/3532001

New Vulnerabilities Tested in SecureScout

❖ 13276 CVS Insecure Temporary File Usage Security Issue

CVS is the Concurrent Versions System, the dominant open-source network-transparent version control system.

Josh Bressers has reported a security issue in cvs, which potentially can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

The security issue is caused due to insecure temporary file usage by the cvsbug.in script when saving temporary output to "/tmp" . This may be exploited via symlink attacks to create or overwrite arbitrary files with the privileges of the user invoking the vulnerable script.

The security issue has been reported in version 1.12.12. Other versions may also be affected.

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

References:

Original advisory:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166366

Other references:
http://secunia.com/advisories/16553/

Product HomePage:
http://www.nongnu.org/cvs/

CVE Reference: CAN-2005-2693

❖ 16113 ProFTPD FTP glob Expansion Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

ProFTPD is vulnerable to a denial of service condition resulting from poor globbing algorithms and user resource usage limits.

Globbing generates pathnames from file name patterns used by the shell, eg. wildcards denoted by * and ?, multiple choices denoted by {}, etc.

The vulnerable FTP servers can be exploited to exhaust system resources if per-user resource usage controls have not been implemented.

The vulnerability affects versions up to 1.2.1.

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

References:

Original Advisory:
http://securityfocus.com/advisories/3456
http://securityfocus.com/advisories/3802

Other references:
http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000450
http://securityfocus.com/bid/2496

Product page:
http://www.proftpd.org/

CVE Reference: None

❖ 16114 ProFTPD SIZE Remote Denial of Service Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

A memory leak has been reported in all versions of ProFTPd.

The SIZE FTP command causes the server to misallocate and leak small amounts of memory each time the command is executed.

If a sufficient number of these commands are executed by the server, substantial amounts of system memory can be consumed, allowing a remote attacker to carry out a denial of service attack on the affected host.

This could be problematic if anonymous FTP is enabled or if a malicious local user has been supplied with an FTP login ID.

The vulnerability affects versions up to 1.2.0.

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

References:

Original Advisory:
http://securityfocus.com/advisories/3102
http://securityfocus.com/advisories/3134
http://securityfocus.com/advisories/3106

Other references:
http://securityfocus.com/bid/2185

Product page:
http://www.proftpd.org/

CVE Reference: CVE-2001-0136

❖ 16115 ProFTPD USER Remote Denial of Service Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

A memory leak has been reported in all versions of ProFTPd.

The USER FTP command causes the server to misallocate and leak small amounts of memory each time the command is executed.

If a sufficient number of these commands are executed by the server, substantial amounts of system memory can be consumed, allowing a remote attacker to carry out a denial of service attack on the affected host.

This could be problematic if anonymous FTP is enabled or if a malicious local user has been supplied with an FTP login ID.

The vulnerability affects versions up to 1.2.0.

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

References:

Original Advisory:
http://securityfocus.com/advisories/3098
http://securityfocus.com/advisories/3134
http://securityfocus.com/advisories/3106

Other references:
http://securityfocus.com/bid/2366

Product page:
http://www.proftpd.org/

CVE Reference: CVE-2001-0136

❖ 16116 ProFTPD setproctitle() Format String Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

A number of ftp daemons, including versions of wu-ftpd, OpenBSD ftpd (ports of this package are distributed with some Linux distributions), HP-UX ftpd, and proftpd, have a vulnerability caused by the passing of user input to the set_proc_title() function. This function in turn calls setproctitle() after using this user data to generate a buffer to pass to setproctitle. setproctitle is defined as setproctitle(char *fmt, ...). The buffer created is passed as the format argument to setproctitle. setproctitle will make a call to the vsnprintf() call, taking the buffer passed as the format string. By carefully manipulating the contents of this buffer, a remote user can cause values on the stack to be overwritten, and potentially cause arbitrary code to be executed as root.

The vulnerability affects versions up to 1.2.0pre10.

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

References:

Original Advisory:
http://securityfocus.com/advisories/2409

http://securityfocus.com/advisories/2390
http://securityfocus.com/advisories/2512
http://securityfocus.com/advisories/2404
http://securityfocus.com/advisories/2397
http://securityfocus.com/advisories/2444

Other references:
http://www.debian.org/security/2000/20000719
http://securityfocus.com/bid/1425

Product page:
http://www.proftpd.org/

CVE Reference: CAN-2000-0574

❖ 16117 ProFTPD snprintf Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

Lack of user input validation in ProFTPD can lead to a remote root vulnerability. On systems that support it ProFTPD will attempt to modify the name of the program being executed (argv[0]) to display the command being executed by the logged on user. It does this by using snprintf to copy the input of the user into a buffer. The call to snprintf is in the 'set_proc_title' function in the main.c source file. It is only compiled in if the define PF_ARGV_TYPE equals the PF_ARGV_WRITABLE define. ProFTPD passes the user input to snprintf as the format argument string of the function call. This allows remote users to supply possible dangerous format arguments to snprintf.

The vulnerability affects versions up to 1.2.0pre6.

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

References:

Original Advisory:
http://securityfocus.com/bid/650

Other references:
http://securityfocus.com/bid/650/ftp.proftpd.net/pub/proftpd

Product page:
http://www.proftpd.org/

CVE Reference: XXXXXXXX

❖ 16118 ProFTPD Remote Buffer Overflow

ProFTPD is an FTP server available for many Unix platforms.

The vulnerability in 1.2pre1, 1.2pre3 and 1.2pre3 is a remotely exploitable buffer overflow, the result of a sprintf() in the log_xfer() routine in src/log.c. The vulnerability in

1.2pre4 is a mkdir overflow. The name of the created path can not exceed 255 chars. 1.2pre6 limits the command buffer size to 512 characters in src/main.c and modifies the fix from 1.2pre4.

The vulnerability affects versions up to 1.2.0pre5.

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

References:

Original Advisory:
http://securityfocus.com/bid/612

Other references:
http://securityfocus.com/bid/612/ftp.proftpd.net/pub/proftpd

Product page:
http://www.proftpd.org/

CVE Reference: CAN-1999-0911

❖ 16119 ProFTPD Long Path Buffer Overflow Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

ProFTPd versions prior to and including 1.2pre1, as well as wuftpd versions up to 2.4.2academ[BETA-18] and 2.4.2 beta 18 vr9 are vulnerable to a buffer overflow that could result in remote root access. The user must have write access and be able to create an unusually long directory or directory structure in order to exploit this buffer overflow. The precise details of this have not been determined, but it is vendor acknowledged.

The vulnerability affects versions up to 1.2.0pre2.

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

References:

Original Advisory:
http://securityfocus.com/advisories/1848
http://securityfocus.com/advisories/517
http://securityfocus.com/advisories/1170

Other references:
http://securityfocus.com/bid/2242

Product page:
http://www.proftpd.org/

CVE Reference: CVE-1999-0368

❖ 16120 ProFTPD realpath Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

There is a vulnerability in ProFTPD versions 1.2.0pre1 and earlier and in wu-ftpd 2.4.2 (beta 18) VR9 and earlier. This vulnerability is a buffer overflow triggered by unusually long path names (directory structures). For example, if a user has write privilages he or she may create an unusually long pathname which due to insuficient bounds checking in ProFTPD will overwrite the stack. This will allow the attacker to insert their own instruction set on the stack to be excuted thereby elavating their access.

The problem is in a bad implementation of the "realpath" function.

The vulnerability affects versions up to 1.2.0pre1.

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

References:

Original Advisory:
http://securityfocus.com/advisories/517
http://securityfocus.com/advisories/611
http://securityfocus.com/advisories/571

Other references:
http://www.debian.org/security/1999/19990210
http://www.netect.com/news19.html
http://securityfocus.com/bid/113

Product page:
http://www.proftpd.org/

CVE Reference: CVE-1999-0368

❖ 17637 Apache 2.x Byte-Range Filter Denial of Service Vulnerability

Filip Sneppe has reported a vulnerability in Apache, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the byte-range filter when handling a request containing the HTTP "Range" header. This can be exploited to cause Apache to consume large amounts of memory.

The vulnerability has been reported in version 2.0.49. Other versions may also be affected.

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

References:

Initial Advisory:
http://issues.apache.org/bugzilla/show_bug.cgi?id=29962

Other references:
http://secunia.com/advisories/16559/

Product Home Page:
http://httpd.apache.org/

CVE Reference: None

New Vulnerabilities found this Week

- **DameWare Mini Remote Control Buffer Overflow Vulnerability**

"Execution of arbitrary code"

Jackson Pollocks No5 has discovered a vulnerability in DameWare Mini Remote Control, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error when handling an overly long user ID. This can be exploited to cause a stack-based buffer overflow and allows execution of arbitrary code.

The vulnerability has been confirmed in version 4.8.0.3, and has been reported to affect all versions above 4.0 and prior to 4.9.0.

References:
http://www.jpno5.com/Releases/Public/Exploits/Dameware%20Mini%20Remote%20Control%20Exploit/dameware.txt

- **Novell NetWare CIFS Denial of Service Vulnerability**

"Denial of Service"

A vulnerability has been reported in NetWare, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in CIFS.NLM when handling password lengths and can be exploited to cause crash the service.

The vulnerability has been reported in NetWare 5.1, 6.0, 6.5 SP2 and 6.5 SP3.

NOTE: The "worm_rbot.ccc" worm, which exploits a Windows vulnerability, may reportedly trigger this vulnerability.

References:
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2971832.htm
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2971821.htm
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2971822.htm

- **mplayer "strf" Header Memory Corruption Vulnerability**

“Compromise a vulnerable system”

Sven Tantau has reported a vulnerability in mplayer, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a error when handling the "strf" stream-format header for audio data and may be exploited to cause a memory corruption via an overly large value in the channel parameter.

The vulnerability has been reported in version 1.0pre7 and prior.

References:
http://www.sven-tantau.de/public_files/mplayer/mplayer_20050824.txt

❖ **Symantec AntiVirus Corporate Edition / Client Security Privilege Escalation**
“Gain escalated privileges”

A vulnerability has been reported in Symantec AntiVirus Corporate Edition and Symantec Client Security, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to the GUI invoking the help functionality insecurely via the "Scan for viruses" option without dropping privileges. This can be exploited to execute arbitrary programs on the system with SYSTEM privileges.

The vulnerability affects the following versions:
* Symantec AntiVirus Corporate Edition 9.0
* Symantec AntiVirus Corporate Edition 9.0.1
* Symantec AntiVirus Corporate Edition 9.0.2
* Symantec Client Security 2.0
* Symantec Client Security 2.0.1
* Symantec Client Security 2.0.2

References:
http://securityresponse.symantec.com/avcenter/security/Content/2005.08.24.html
http://www.idefense.com/application/poi/display?id=298&type=vulnerabilities

❖ **Apache Byte-Range Filter Denial of Service Vulnerability**
“Denial of Service”

Filip Sneppe has reported a vulnerability in Apache, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the byte-range filter when handling a request containing the HTTP "Range" header. This can be exploited to cause Apache to consume large amounts of memory.

The vulnerability has been reported in version 2.0.49. Other versions may also be affected.

References:
http://issues.apache.org/bugzilla/show_bug.cgi?id=29962

❖ **Linux Kernel Denial of Service and IPsec Policy Bypass**

"Denial of Service; bypass certain security restrictions"

Two vulnerabilities have been reported in the Linux kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or bypass certain security restrictions.

1) The "setsockopt()" function is not restricted to privileged users with the "CAP_NET_ADMIN" capability. This can be exploited to bypass IPsec policies or set invalid policies to exploit other vulnerabilities or exhaust available kernel memory.

2) An error in the "syscall32_setup_pages()" function on 64-bit x86 platforms can be exploited to cause a memory leak by executing a malicious 32-bit application with specially crafted ELF headers.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.13

❖ **CVS Insecure Temporary File Usage Security Issue**

"Escalated privileges"

Josh Bressers has reported a security issue in cvs, which potentially can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

The security issue is caused due to insecure temporary file usage by the cvsbug.in script when saving temporary output to "/tmp" . This may be exploited via symlink attacks to create or overwrite arbitrary files with the privileges of the user invoking the vulnerable script.

The security issue has been reported in version 1.12.12. Other versions may also be affected.

References:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=166366

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