netVigilance

ScoutNews Team **August 26, 2005**
Issue # 34

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Intel makes showing in network security, CA suffers more exploit woes, hacker scores direct hit on USAF data, whitehats collar MSN hacker and Microsoft suffers another virus outbreak – **Measles** !?

Enjoy reading and stay safe.

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

Top Security News Stories this Week

- **Intel announces anti-worm technology**

Justin Rattner, director of Intel corporate technology announced at the Intel Developers Forum (IDF) this week, the existence of a "system" called CircuitBreaker that detects possible worm activity in a computer then shuts down it's network connections.

Rattner then demonstrated Circuit Breaker. This Intel research project stops worms by enabling each device to intelligently monitor the health of its own network traffic - effectively stopping a worm in its tracks before the user is even aware there is a problem. "By the time humans know there is a problem, it's too late," said Rattner. User-aware computers could heal themselves saving individuals and industry time and money.

Related Links:

http://www.ebcvg.com/articles.php?id=857
http://www.intel.com/idf/us/fall2005/about/keynotes_review.htm#rattner

- **More holes found in CA applications**

Computer Associates disclosed the existence of vulnerabilities in it's CA Message (CAM) Queuing software, which could allow hackers to launch DoS attacks against servers running the software.

Earlier in the year SC Magazine reported on a number of vulnerabilities affecting security products from CA, Trend Micro and Check Point.

SC Magazine

Full Story :
http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=961627b6-45b5-42d2-a04c-b1b48701f6fe&newsType=News

- **33,000 Air Force personnel records at risk from hack**

A hacker gained access to US Air Force database the holds Social Security numbers and other personal information on 33,000 officers and enlisted personne,l about half of the officers in the Air Force.

No identity theft has been reported at press time; On Friday 8/19, the people affected were notified of steps they can take to protect their identity.

Associated Press

Related Links:
http://news.yahoo.com/s/ap/20050823/ap_on_go_ca_st_pe/military_records_accessed

- **MSN Phisher arrested**

FBI agents and local police in Davenport, Iowa, arrested Jayson Harris, 22, and charged him with 75 counts of wire fraud for allegedly stealing credit card numbers and personal information in a phishing (define) scheme targeting Microsoft's (Quote, Chart) MSN customers.

.internetnews.com

Related Links:
http://www.internetnews.com/security/article.php/3529746
http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=59837

- **Microsoft hit by Measles outbreak**

Health officials in Washington State have issued a warning of a virus outbreak on the Microsoft campus at Redmond. one confirmed case of measles in an adult traveler who acquired the disease abroad. The infected person visited public areas in King County while contagious and may have exposed other persons to the disease. I've got my shots – Ed.

KING COUNTY, WASHINGTON - Public Health

Related Link:
http://www.metrokc.gov/health/news/05082501.htm

New Vulnerabilities Tested in SecureScout

- **15227 Adobe Acrobat / Reader Plug-in Buffer Overflow Vulnerability (Remote File Checking)**

A vulnerability has been reported in Adobe Reader and Adobe Acrobat, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified boundary error in the core application plug-in and can be exploited to cause a buffer overflow when a specially crafted file is opened.

Successful exploitation may allow execution of arbitrary code.

The issue has been fixed in the following versions:

Adobe Reader (Windows or Mac OS):
Update to version 7.0.3 or 6.0.4.

Adobe Acrobat (Windows or Mac OS):
Update to version 7.0.3, 6.0.4, or 5.0.10.

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

References:

Original advisories:
http://www.adobe.com/support/techdocs/321644.html

Other references:
http://www.kb.cert.org/vuls/id/896220
http://secunia.com/advisories/16466/

Product HomePage:
http://www.adobe.com/products/

CVE Reference: CAN-2005-2470

❖ 15756 Microsoft DDS Library Shape Control Code Execution Vulnerability (906267) (Remote File Checking)

A vulnerability has been reported in Internet Explorer, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error when the "msdds.dll" (Microsoft DDS Library Shape Control) COM object is instantiated in the Internet Explorer browser.

Successful exploitation allows execution of arbitrary code, but requires that a user is tricked into visiting a malicious web site.

Vulnerable versions of the COM object (versions 7.0.9064.9112 and 7.0.9446.0) are installed as part of the following products:
* Microsoft Visual Studio 2002
* Microsoft Access 2002
* Microsoft Office XP

According to Microsoft, later versions of the COM object (e.g. included with Microsoft Office 2003 and Microsoft Visual Studio .NET 2003) are not vulnerable.

NOTE: An exploit has been published

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

References:

Original Advisory:
Microsoft (KB906267):
http://www.microsoft.com/technet/security/advisory/906267.mspx
http://support.microsoft.com/kb/906267

Other References:
ISC:
http://isc.sans.org/diary.php?date=2005-08-18

US-CERT VU#740372:
http://www.kb.cert.org/vuls/id/740372

Secunia:
http://secunia.com/advisories/16480/

CVE Reference: CAN-2005-2127

❖ 16105 ProFTPD CIDR Access Control Rule Bypass Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

ProFTPD has been reported prone to an access control rule bypass vulnerability. The issue was reportedly introduced when a "portability workaround" was applied to

ProFTPD version 1.2.9.

This vulnerability may lead a system administrator into a false sense of security, where it is believed that access to the ProFTPD server is restricted by access control rules. In reality the access control restriction will not be enforced at all.

The vulnerability affects version 1.2.9

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

References:

Original Advisory:
http://securityfocus.com/advisories/6728

Other references:
http://securityfocus.com/advisories/6651
http://securityfocus.com/advisories/6647
http://securityfocus.com/advisories/6648
http://securityfocus.com/bid/10252

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

CVE Reference: CAN-2004-0432

❖ 16106 ProFTPD _xlate_ascii_write() Buffer Overrun Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

A remotely exploitable buffer overrun was reported in ProFTPD. This issue is due to insufficient bounds checking of user-supplied data in the _xlate_ascii_write() function, permitting an attacker to overwrite two bytes memory adjacent to the affected buffer. This may potentially be exploited to execute arbitrary code in the context of the server. This issue may be triggered when submitting a RETR command to the server.

The vulnerability affects version up to 1.2.9rc2.

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

References:

Original Advisory:
http://support.coresecurity.com/impact/exploits/68df523e66c168ffb6f2a30bee6cd120.html

Other references:
http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raqxtr.eng&nav=patchpage
http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq4.eng&nav=patchpage
http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/qube3.eng&nav=patchpage
http://securityfocus.com/archive/1/355933

http://securityfocus.com/bid/9782

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

CVE Reference: CAN-2004-0346

❖ 16107 ProFTPD SQL Injection mod_sql Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

ProFTPD has been reported prone to SQL injection attacks. Specifically, ProFTPD versions that use the mod_sql module to manipulate PostgreSQL databases are prone to SQL injection attacks. The vulnerability occurs due to insufficient sanitization of user-supplied data when logging onto the FTP server.

Successful exploitation may result in an attacker obtaining privileged access to the FTP server. Other attacks are also possible.

The vulnerability affects version up to 1.2.9rc1.

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

References:

Original Advisory:
http://securityfocus.com/advisories/5517
http://securityfocus.com/advisories/5538

Other references:
http://securityfocus.com/bid/7974

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

CVE Reference: None

❖ 16108 ProFTPD 1.2.0rc2 log_pri() Format String Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

A vulnerability exists in ProFTPD when executing its shutdown routine. It has been reported that the main_exit() called during shutdown fails to sufficiently supply format specifiers for input. Under certain circumstances the input passed to the function may contain user-supplied input.

If this format bug were successfully exploited, an attacker may be able to create a situation in which arbitrary code execution may occur.

The vulnerability affects version up to 1.2.0rc3.

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

References:

Original Advisory:
http://securityfocus.com/advisories/3102
http://securityfocus.com/advisories/3130
http://securityfocus.com/advisories/3106

Other references:
http://securityfocus.com/bid/6781

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

CVE Reference: CVE-2001-0318

❖ 16109 ProFTPD Server Virtual User File Removal Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

Under some circumstances, it may be possible for users to remove files that have been placed in an FTP archive by other users. A file placed by one user may be delete by another user with insufficient permissions, though the target file may not be overwritten. This problem has been reported to occur in the instance of the virtual user feature of FTP servers being used on Solaris systems.

The vulnerability affects version 1.2.7.

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

References:

Original Advisory:
http://securityfocus.com/archive/1/307655

Other references:
http://securityfocus.com/bid/6649

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

CVE Reference: None

❖ 16110 ProFTPD STAT Command Denial Of Service Vulnerability

A denial of service vulnerability has been reported for ProFTPD. It is possible to cause ProFTPD from responding to legitimate requests for service by issuing specially crafted STAT commands. This will result in a denial of service condition.

The vulnerability affects versions up to 1.2.7rc3.

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

References:

Original Advisory:
http://securityfocus.com/archive/1/302779

Other references:
http://securityfocus.com/bid/6341

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

CVE Reference: XXXXXXXX

❖ 16111 ProFTPD mod_sqlpw Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

Compiling the mod_sqlpw module into ProFTPD makes it possible for local users to view the passwords of users who have connected to the ftp server. When the module is used, it writes information to wtmp. Unfortunately, it writes the password to wtmp where the username should be. The passwords can be seen when a command such as 'last' is used locally.

The vulnerability affects versions up to 1.2.1.

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

References:

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

Other references:
http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000450
http://securityfocus.com/bid/812

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

CVE Reference: CAN-1999-1475

❖ 16112 ProFTPD Client Hostname Resolving Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

ProFTPD contains a vulnerability which may allow for remote attackers to bypass ProFTPD access control lists or have false information logged. ProFTPD does not forward resolve reverse-resolved hostnames to verify that the IP address matches of the client matches DNS records.

It may be possible for a remote attacker with control over address space to set an

arbitrary hostname as the PTR record for the attacking address. This false hostname will be evaluated against the ProFTPD ACLs and recorded in log files.

The vulnerability affects versions up to 1.2.2.

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

References:

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

Other references:
http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000450
http://securityfocus.com/bid/3310

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

CVE Reference: None

New Vulnerabilities found this Week

- **Symantec AntiVirus Corporate Edition / Client Security Privilege Escalation**

"Local users to 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 without dropping privileges, which can be exploited to gain SYSTEM privileges on a vulnerable system.

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

- **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"

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/testing/ChangeLog-2.6.13-rc7
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.13-rc4

❖ **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

❖ **Sun Solaris DHCP Client Arbitrary Code Execution Vulnerability**

"Execute arbitrary code"

A vulnerability has been reported in Solaris, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error in the "/lib/svc/method/net-svc" script and can be exploited to execute arbitrary code on a DHCP client with root privileges.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101897-1

❖ **pam_ldap Client Authentication Security Bypass**

"Bypass certain security restrictions"

A security issue has been reported in pam_ldap, which can be exploited by malicious people to bypass certain security restrictions.

The problem is caused due to an error when a pam_ldap client authenticates against an LDAP server that returns a passwordPolicyResponse control in a BindResponse without the optional "error" field.

Successful exploitation grants access without checking the authentication result.

The security issue has been reported in versions 169 through 179.

References:
http://www.kb.cert.org/vuls/id/778916

❖ **Microsoft IIS "500-100.asp" Source Code Disclosure**

"Gain knowledge of potentially sensitive information"

Inge Henriksen has discovered a vulnerability in Microsoft Internet Information Services (IIS), which can be exploited by malicious people to gain knowledge of potentially sensitive information.

The vulnerability is caused due the "500-100.asp" script making assumptions based on the user-controlled "SERVER_NAME" variable. This can be exploited to gain knowledge of script contents when an error is encountered via a specially crafted HTTP request.

The vulnerability has been confirmed in IIS 5.1 and has also been reported in

versions 5.0 and 6.0.

References:
http://ingehenriksen.blogspot.com/2005/08/remote-iis-5x-and-iis-60-server-name.html

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