netVigilance

ScoutNews Team **17 September 2004**
Issue #38

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Hardware manufacturers like IBM are trying to improve security at the physical layer or right above it and people are losing there jobs in a high profile security incident.
However the most important news this week is that Vulnerability related down time will increase three fold over the next three years for security lax companies. Gartner says you need to be proactive in your vulnerability management in order to avoid this impact.
At the same time we see the proof of this threat as hackers flock around the latest Microsoft flaws.

Enjoy reading

Top Security News Stories this Week

- **IBM Builds In PC Security**
  SafeKeeper module stores passwords, encryption keys in ThinkCentre desktops.
  National Semiconductor's SafeKeeper Trusted I/O devices add to its existing chip design a "trusted platform module", a microcontroller that stores passwords, digital certificates, and encryption keys. The devices conform to the TPM specifications developed by the Trusted Computing Group, a 2-year-old standards body for hardware-based security technologies backed by IBM, Intel, Advanced Micro Devices, Microsoft, and Hewlett-Packard.
  The idea behind hardware-based security is that information stored in a PC's firmware is less vulnerable to attack than data protected only by software. TPM-stored data can, for instance, be used to authenticate a computer on a network, providing identity information in a way that's harder to forge.

http://www.pcworld.com/news/article/0,aid,117820,00.asp
Stacy Cowley

- **Five lose jobs over nuke lab security debacle**
  Los Alamos National Laboratory has fired four workers and another employee is to resign over a security scandal that resulted in the top secret lab suspending classified work.
  The fired workers were among 23 suspended in July after two disks containing classified information went missing and an intern was injured in an accident with a laser. Three of

the workers will leave over the disc debacle, while two have been shown the door over breaches in health and safety procedures that led to the laser incident.

http://www.theregister.co.uk/2004/09/16/los_alamos_sackings/

John Leyden

- **Downtime Will Triple For Security-Lax Firms**

  Enterprises that don't take proactive security steps will see their vulnerability-caused downtime triple in the next five years, a research firm said Monday.

  In a just-released report, Gartner research fellow John Pescatore estimated that the current five percent of downtime attributed to security vulnerabilities will grow to 15 percent by 2008 unless firms work on security in their own development, and demand highly-secure software when they purchase commercial software.

http://www.internetweek.com/breakingNews/showArticle.jhtml;jsessionid=YAAKSKYYWCZ3GOQSNDBCCKHQ?articleID=47204631

TechWeb News

- **Hackers Jump On Windows Vulnerability**

  Hackers are drooling at the thought of exploiting Microsoft's most recent vulnerabilities, security analysts said Thursday.

  Less than 24 hours after Microsoft released details of the latest vulnerability in Windows, hackers were sharing details and eager to get their hands on exploit code, said Ken Dunham, the director of malicious code research for Reston, Va.-based security intelligence provider iDefense.

http://www.internetweek.com/breakingNews/showArticle.jhtml%3Bjsessionid=T0JURY3ATJOTMQSNDBCCKHY?articleID=47212311

Gregg Keizer, TechWeb News

New Vulnerabilities Tested in SecureScout

- **14041 Samba ASN.1 Parsing Function Malformed Request DoS 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.

  Samba contains a flaw that may allow a remote denial of service. The issue is triggered when an attacker sends specially crafted packets to the smbd daemon during the ASN.1 parsing routine causing many processes to spawn resulting in a loss of availability for the platform.

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

CVE Links: CAN-2004-0807

Reference: http://www.idefense.com/application/poi/display?id=139&type=vulnerabilities & http://us3.samba.org/samba/history/3.0_DOS_sept04_announce.txt & http://www.samba.org

- **14042 Samba nmbd process_logon_packet Function DoS 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.

  Samba contains a flaw that may allow a remote denial of service. The issue is triggered when an attacker sends a malformed UDP packet and will result in loss of availability for Samba's nmbd daemon. The process_logon_packet function does not properly validate that the packet is appropriately sized to contain the number of structures it claims, when processing a SAM_UAS_CHANGE request. If the packet claims a large number of structures and a smaller number are contained in the packet, nmbd will reference memory outside of the packet, possibly causing the daemon to crash.

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

CVE Links: CAN-2004-0808

Reference: http://www.idefense.com/application/poi/display?id=138&type=vulnerabilities & http://www.samba.org

- **14043 Samba Mangling Method Hash 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.
  Samba contains a flaw related to the "mangling method = hash" option that may allow an attacker to cause a buffer overflow. No further details have been provided.

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

CVE Links: CAN-2004-0686

Reference: http://www.samba.org

- **15078 Microsoft XP Service Pack 2 not installed (Registry Check)**
  Microsoft Service Pack 2 has been made available by Microsoft in order to fix a lot of security issues affecting Windows XP.
  It is recommended that you apply Service Pack 2 on the host.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://support.microsoft.com/default.aspx?scid=fh;ln;xpsp2getinstall

- **15127 DNS server allows recursion**
  A major concern with DNS servers is called Cache Poisoning. This is a direct consequenence of DNS servers allowing recursion.

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

CVE Link: CVE-1999-0024

Reference: http://www.jhsoft.com/help/index.html?df_recursion.htm & http://www.oreilly.com/catalog/dns4/chapter/ch11.html & http://www.securityfocus.com/guest/17905 & http://www.securityfocus.com/bid/678

- 15528 **Cisco 6000/6500/7600 Crafted Layer 2 Frame Vulnerability**

(CSCdy15598/CSCeb56052)

A layer 2 frame that is encapsulating a protocol independent layer 3 packet (IP, IPX, etc.) may cause Cisco 6000/6500/7600 series systems with an MSFC2 to freeze or reset. The actual length of the layer 2 frame needs to be inconsistent with the length of the encapsulated layer 3 packet.

A layer 3 packet that is routed by the Cisco 6000/6500/7600 series systems may trigger this vulnerability if the packet is encapsulated in a specifically crafted layer 2 frame. Crafted packets must be software switched on the vulnerable systems to trigger this vulnerability. The packets that are switched in hardware will not trigger this vulnerability. Although such frames can only be sent from the local network segment, there might be some cases where it is possible to trigger this vulnerability remotely. For remote exploitation, the crafted layer 2 frames need to pass through all the intermediate layer 3 devices between the source and the destination without being clipped. Remote exploitation will not be possible even if only a single layer 3 device on the path from source to destination clips the crafted layer 2 frame. To the best of our knowledge, only Cisco 6000/ 6500/7600 series will forward such crafted frames without being corrected.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20040203-cat6k.shtml & http://www.securityfocus.com/bid/9562

❖ 15817 Cisco Scanning for SSH Can Cause a Crash (CSCdv85279/CSCdw59394)

While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities (http://www.cisco.com/warp/public/707/SSH-multiple-pub.html) Cisco inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.

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

CVE Link: CVE-2002-1024

Reference: http://www.cisco.com/warp/public/707/SSH-scanning.shtml

❖ 17921 Apache 2 apr-util Library and Environment Variable Expansion Vulnerabilities

Two vulnerabilities have been reported in Apache, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a system, or by malicious, local users to gain escalated privileges.

1) An input validation error within the apr-util library's IPv6 URI parsing functionality can be exploited via a specially crafted request.

Successful exploitation crashes a httpd child process. However, it is reportedly believed that the vulnerability may allow code execution on BSD systems.

The vulnerability affects versions 2.0.35 through 2.0.50.

2) A boundary error within the expansion of environment variables when parsing

configuration files can be exploited to cause a buffer overflow via a specially crafted ".htaccess" file.
Successful exploitation may allow a malicious, local user to gain escalated privileges.
The vulnerability affects versions 2.0.35 through 2.0.50.

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

CVE Link: CAN-2004-0747 & CAN-2004-0786

Reference: http://www.uniras.gov.uk/vuls/2004/403518/index.htm

- **17922 Apache 2 "mod_dav" LOCK Request Denial of Service Vulnerability**
  A vulnerability has been reported 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 "mod_dav" module. A malicious client can exploit this to crash an httpd child process by sending a particular sequence of LOCK requests.
  Successful exploitation requires that the malicious client is allowed to use the LOCK method and the threaded process model is used.

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

CVE Link: CAN-2004-0809

Reference: http://httpd.apache.org/download.cgi

- **17923 Apache 2 "mod_ssl" Denial of Service Vulnerabilities**
  Two vulnerabilities have been reported in Apache 2 mod_ssl, which can be exploited by malicious people to cause a DoS (Denial of Service).
  1) It is possible to cause mod_ssl to enter an infinite loop by aborting a SSL connection in a particular state. This causes the process to consume large amounts of CPU resources.
  2) An error in mod_ssl when running in "speculative" mode can be exploited to cause an access violation via e.g. a proxy request to a remote SSL server.
  The vulnerabilities have been reported in Apache 2.0.50 and prior.

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

CVE Link: CAN-2004-0748 & CAN-2004-0751

Reference: http://httpd.apache.org/download.cgi

New Vulnerabilities found this Week

- **Microsoft Office WordPerfect Converter Buffer Overflow Vulnerability**

“Execution of arbitrary code”

Peter Winter-Smith has reported a vulnerability in various Microsoft Office products, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error within the WordPerfect Converter and can be exploited to cause a buffer overflow if a user opens a malicious document.

Successful exploitation may allow execution of arbitrary code with the users privileges.
The vulnerability affects WordPerfect Converter 5.x, which is included in various Microsoft Office products.
References: http://www.microsoft.com/technet/security/bulletin/ms04-027.mspx

- **Microsoft Multiple Products JPEG Processing Buffer Overflow Vulnerability**

"Execution of arbitrary code"
Nick DeBaggis has reported a vulnerability in multiple Microsoft products, which can be exploited by malicious people to compromise a user's system.
The vulnerability in caused due to a boundary error within the GDI+ JPEG Parsing component (Gdiplus.dll). This can be exploited to cause a buffer overflow by tricking a user into viewing a specially crafted JPEG image with any application using the vulnerable component for JPEG image processing.
Successful exploitation allows execution of arbitrary code with the privileges of the user.

References: http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx

- **X11 libXpm XPM Image Decoding Vulnerabilities**

"Execution of arbitrary code"
Chris Evans has reported multiple vulnerabilities in libXpm, which potentially can be exploited by malicious people to compromise a vulnerable system.
1) A boundary error within the "xpmParseColors()" function can be exploited to cause a stack-based buffer overflow when a specially crafted XPM file is processed.
Successful exploitation may potentially allow execution of arbitrary code.
2) Various input validation errors can be exploited to cause integer overflows when a specially crafted XPM file is processed.
Successful exploitation causes an affected application to crash and may potentially also allow arbitrary code execution.

References: http://www.x.org/pub/X11R6.8.0/p...ME.xorg-CAN-2004-0687-0688.patch

- **GNU Radius SNMP String Length Denial of Service Vulnerability**

"Denial of Service"
A vulnerability has been reported in GNU Radius, which can be exploited by malicious people to cause a DoS (Denial of Service).
The vulnerability is caused due to an input validation error within the "asn_decode_string()" function. This can be exploited to cause an integer overflow and thereby crash the radius daemon by sending a specially crafted SNMP datagram to a vulnerable system.
Successful exploitation requires that radiusd has been compiled with the "--enable-snmp" option (not default setting).
The vulnerability has been reported in versions 1.1 and 1.2.

References: http://www.idefense.com/applicat...?id=141&type=vulnerabilities

- **Mozilla Multiple Vulnerabilities**

"Execution of arbitrary code"
Details have been released about several vulnerabilities in Mozilla, Mozilla Firefox, and Thunderbird. These can potentially be exploited by malicious people to conduct cross-site scripting attacks, access and modify sensitive information, and compromise a user's system.

1) Various boundary errors in "nsMsgCompUtils.cpp" can be exploited to cause heap-based buffer overflows when a specially crafted e-mail is forwarded.
Successful exploitation can potentially lead to execution of arbitrary code.
2) Insufficient restrictions on script generated events on text fields can be exploited to read and write content from and to the clipboard.
3) Boundary errors in the "writeGroup()" function in "nsVCardObj.cpp" can be exploited to cause stack-based buffer overflows by sending an e-mail containing a specially crafted vcard.
Successful exploitation may allow execution of arbitrary code but requires that the malicious e-mail is opened in preview.
4) Some boundary errors in "nsPop3Protocol.cpp", which handles POP3 mail communication, can be exploited to cause buffer overflow by a malicious POP3 mail server when sending specially crafted responses.
Successful exploitation may potentially allow execution of arbitrary code.
5) A problem with overly long links containing a non-ASCII characters can be exploited via a malicious website or e-mail to cause a buffer overflow, which potentially can lead to execution of arbitrary code.
6) An integer overflows when parsing and displaying BMP files can potentially be exploited to execute arbitrary code by supplying an overly wide malicious BMP image via a malicious website or in an e-mail.
7) Mozilla allows dragging links to another window or frame. This can e.g be exploited by tricking a user on a malicious website to drag a specially crafted javascript link to another window.
Successful exploitation can cause script code to execute in context of that window. Further exploitation can in combination with another unspecified vulnerability lead to execution of arbitrary code.
8) Signed scripts can request enhanced privileges, which requires that a user accepts a security dialog. The problem is that a malicious website can pass a specially crafted parameter making it possible to manipulate information displayed in the security dialog.
Successful exploitation allows a website to trick users into accepting security dialogs, which will grant access to run arbitrary programs.
9) Some files installed with the Linux installer are group and world writable. This can be exploited by malicious, local users to replace files, which can lead to execution of arbitrary code.
10) Many files and directories in the Linux install ".tar.gz" archives have wrong owner and permissions. This can be exploited by malicious, local users to replace files if the umask is set to be ignored when unpacking.
Successful exploitation can lead to execution of arbitrary code.
These vulnerabilities reportedly affect versions prior to the following:
- Mozilla 1.7.3
- Firefox 1.0PR
- Thunderbird 0.8

References: http://bugzilla.mozilla.org/show_bug.cgi?id=258005

❖ Samba Denial of Service Vulnerabilities

“Denial of Service”

Two vulnerabilities have been reported in Samba, which can be exploited by malicious people to cause a DoS (Denial of Service).
1) An error exists in smbd within the ASN.1 parsing functionality. This can be exploited via specially crafted packets during authentication to spawn many new processes, which enter infinite loops.
Successful exploitation may exhaust all available memory resources.

2) An input validation error exists in nmbd within the "process_logon_packet()" function when processing mailslot packets. This can be exploited to crash the daemon via a specially crafted "SAM_UAS_CHANGE" request.
Successful exploitation requires that the daemon has been configured to process domain logons ("domain logons = yes" in smb.conf).
The vulnerabilities affect version 3.0.6 and prior.

References: http://us3.samba.org/samba/history/3.0_DOS_sept04_announce.txt

- **McAfee VirusScan System Scan Privilege Escalation Vulnerability**

“Gain escalated privileges”
Ian Vitek has reported a vulnerability in McAfee VirusScan, which can be exploited by malicious, local users to gain escalated privileges on a vulnerable system.
The vulnerability is caused due to the process not dropping its privileges before accessing the "System Scan" properties via the system tray, which makes it possible to execute an arbitrary program with these privileges.
Successful exploitation allows execution of arbitrary commands with SYSTEM privileges.
The vulnerability has been reported in version 4.5.1. Prior versions may also be affected.

References: http://www.idefense.com/applicat...?id=140&type=vulnerabilities

- **Squid "clientAbortBody()" Denial of Service Vulnerability**

“Denial of Service”
M.A.Young has reported a vulnerability in Squid, which can be exploited by malicious people to cause a DoS (Denial of Service).
The vulnerability is caused due to a NULL pointer dereference error within the "clientAbortBody()" function. This can potentially be exploited to crash Squid by visiting a malicious website via the proxy.

References: http://www.squid-cache.org/bugs/show_bug.cgi?id=972

- **Multiple BEA Systems WebLogic Vulnerabilities**

“Unauthorized access, information disclosure”
BEA Systems has released advisories to address multiple vulnerabilities in WebLogic Server and Express. These issues may permit unauthorized access, information disclosure, or pose threats to role and policy security.

References: http://www.securityfocus.com/bid/11168/discussion/

- **ZyXEL P681 ARP Request Information Disclosure Vulnerability**

“Information disclosure”
It is reported that ZyXEL Prestige 681 SDSL routers are susceptible to an information disclosure vulnerability.
An attacker sniffing network traffic on an attached network would be able to retrieve partial contents of network packets that have traversed the affected device.
This information may assist malicious users in attacks on systems and services that utilize the affected device.
ZyNOS version Vt020225a is reported vulnerable to this issue. Due to code reuse among products, it is likely that other devices and versions are also affected by this issue.

References: http://www.securityfocus.com/bid/11167/discussion/

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