netVigilance

ScoutNews Team **24 July 2004**
Issue #30

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The danger of using open source freeware tools when securing your network or in security practices is highlighted in this week's vulnerability in Nessus.

IPv6 offers better security and pays itself back within a year and of course adds a lot more value in wireless networks.

A $40K settlement and you are off the hook as spammer king and can clam innocence. On the other hand the largest yet case of personal data theft from Axiom is started this week.

The window between vulnerability discovery and exploit code release is continuously shrinking – This time there was a week from discovery to release – it seems like we are getting closer and closer to a real nasty Zero day event.

Enjoy reading

Top Security News Stories this Week

❖ **Nessus "adduser" Race Condition Vulnerability**
Cyrille Barthelemy has reported a vulnerability in Nessus, potentially allowing malicious users to escalate their privileges.
The problem is caused by a race condition in "nessus-adduser" if the user hasn't specified the environment variable "TMPDIR".
This has been reported to affect version 2.0.11. Prior versions may also be affected.
http://secunia.com/advisories/12127/
Secunia

❖ **IPv6 Offers Better Security, Wireless Features**
IPv6 enables host machines to automatically discover information (such as the address of a local router) needed to connect to the Internet or corporate IP backbone. Forrester Research says this feature alone will eliminate so much manual configuration, it will pay back the cost of converting to IPv6-based technology within

a year.
Some consider it the best thing since sliced bread. Others dismiss it as a passing fad. The controversy over Internet Protocol version 6 (IPv6) is nowhere near being resolved.
The specification was completed in 1997 by the Internet Engineering Task Force (IETF) as a fix to IPv4 shortcomings, mainly the fact that it's limited to about a billion user addresses.
With the slashing of enterprise technology budgets and continuing distress in the telecom sector, many are understandably asking: "does one really need IPv6?"
http://www.technewsworld.com/story/35269.html
ECT News Syndication Desk

❖ **Man Charged With Hacking Acxiom Database Company**

A Florida man has been charged with stealing large amounts of consumer information from Acxiom Corp., one of the world's largest database companies.
The new indictment comes on the heels of a separate case last year in which an Ohio man pleaded guilty to hacking into an Acxiom server. Acxiom manages personal information on millions of consumers, along with financial and other internal data for companies.
The new case, against Scott Levine, 45, represents "what may be the largest cases of intrusion of personal data to date," U.S. Assistant Attorney General Christopher A. Wray said Wednesday at a news conference in Washington.
http://www.crn.com/sections/breakingnews/dailyarchives.jhtml%3Bjsessionid=DMIYDPDJS1SWSQSNDBGCKHQ?articleId=23904831
Caryn Rousseau

❖ **Windows 2000 Exploit Code Released**

Exploit code for a known security flaw in Microsoft Windows 2000 has been posted online, putting millions of users at risk of a PC hijack.
Less than a week after Microsoft released a fix for an "important" privilege elevation vulnerability in the Windows 2000 Utility Manager feature, hackers have reverse-engineered the patch and released the code that could lead to an exploit.
Microsoft confirmed that the vulnerability could allow a logged-on user to misuse the Utility Manager to start an application with system privileges and take control of the system.
"An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges," the company warned.
http://www.serverwatch.com/news/article.php/3384861
Ryan Naraine

❖ **Spammer to pay $40,000**

High-profile email marketer Scott Richter, aka the 'Spam King', has agreed to pay $40,000 in settlement of a lawsuit brought against him by the State of New York - a mere drop in the ocean compared to the $20 million judgment NY State has initially sought.
Richter, who also agreed to pay $10,000 in investigative costs, has promised to keep records of his business and make them available to the attorney general, but – despite

agreeing to the settlement - he still denies any violations of the law on his part.
http://www.virusbtn.com/news/latest_news/spamking220704.xml
Virus Bulletin Ltd

New Vulnerabilities Tested in SecureScout

- **14453 Cumulative Security Update for Outlook Express (MS04-018/823353)**

This update resolves a public vulnerability. A denial of service vulnerability exists in Outlook Express because of a lack of robust verification for malformed e-mail headers. The vulnerability is documented in the Vulnerability Details section of this bulletin. This update also changes the default security settings for Outlook Express 5.5 Service Pack 2 (SP2).

If a user is running Outlook Express and receives a specially crafted e-mail message, Outlook Express would fail. If the preview pane is enabled, the user would have to manually remove the message, and then restart Outlook Express to resume functionality.

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

CVE Links: CAN-2004-0215

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-018.mspx

- **14454 Vulnerability in Utility Manager Could Allow Code Execution (MS04-019/842526)**

This update resolves a newly-discovered, privately reported vulnerability. A privilege elevation vulnerability exists in the way that Utility Manager launches applications. A logged-on user could force Utility Manager to start an application with system privileges and could take complete control of the system.

An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

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

CVE Links: CAN-2004-0213

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-019.mspx

- **14455 Vulnerability in POSIX Could Allow Code Execution (MS04-020/841872)**

This update resolves a newly-discovered, privately reported vulnerability. A privilege elevation vulnerability exists in the POSIX operating system component (subsystem).

An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

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

CVE Links: CAN-2004-0210

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-020.mspx

- **14456 Security Update for IIS 4.0 (MS04-021/841373)**

This update resolves a newly-discovered, privately reported vulnerability.

A buffer overrun vulnerability exists in Internet Information Server 4.0 that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

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

CVE Link: CAN-2004-0205

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-021.mspx

- **14457 Vulnerability in Task Scheduler Could Allow Code Execution (MS04-022/841873)**

This update resolves a newly-discovered, privately reported vulnerability. A remote code execution vulnerability exists in the Task Scheduler because of an unchecked buffer.

If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. However, user interaction is required to exploit this vulnerability. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Link: CAN-2004-0212

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-022.mspx

- **14458 Vulnerability in HTML Help Could Allow Code Execution (MS04-023/840315)**

This update resolves two newly-discovered vulnerabilities. The HTML Help vulnerability was privately reported and the showHelp vulnerability is public.

If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts

that have full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Link: CAN-2003-1041 & CAN-2004-0201

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-023.mspx

- **14459 Vulnerability in Windows Shell Could Allow Remote Code Execution (MS04-024/839645)**

This update resolves a newly-discovered, publicly reported vulnerability. A remote code execution vulnerability exists in the way that the Windows Shell launches applications.

If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. However, significant user interaction is required to exploit this vulnerability. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Link: CAN-2004-0420

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-024.mspx

- **17562 CGI SAPI of PHP version 4.3.0 Vulnerability**

PHP contains code for preventing direct access to the CGI binary with configure option "--enable-force-cgi-redirect" and php.ini option "cgi.force_redirect". In PHP 4.3.0 there is a bug which renders these options useless. Anyone with access to websites hosted on a web server which employs the CGI module may exploit this vulnerability to gain access to any file readable by the user under which the webserver runs.
A remote attacker could also trick PHP into executing arbitrary PHP code if attacker is able to inject the code into files accessible by the CGI.

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

CVE Link: CAN-2003-0097

Reference: http://marc.theaimsgroup.com/?l=bugtraq&m=104550977011668&w=2 & http://www.php.net

- **17907 phpMyAdmin Input Validation Errors in 'left.php' PHP Code Injection Vulnerability**

phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW.

There is a vulnerability in phpMyAdmin version 2.5.7. and earlier.
This vulnerability would allow remote user to inject

php codes to be executed by eval() function (in file left.php).
However, This vulnerability only effect if variable
$cfg['LeftFrameLight'] set to FALSE (in file config.inc.php).

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://eagle.kecapi.com/sec/fd/phpMyAdmin.html &
http://eagle.kecapi.com/sec/codes/phpmy-expt.c &
http://securitytracker.com/alerts/2004/Jun/1010614.html & www.phpmyadmin.net/home_page/

- **19056 Hijack ISTbar**

Installed by ActiveX drive-by download on affiliate sites; typically porn in the case of XXXToolbar. ISTbar/MSCache was widely distributed to users clicking links to the 'OutWar' online game. ISTbar/AUpdate is known to install using aggressive JavaScript (opening an error and retrying if you refuse the ActiveX download).

Variants install other third-party software which includes advertising. The XXXToolbar variant opens pop-ups as directed by its controlling server. In AUpdate, the TinyBar component could be used to open pop-ups in the future. All versions also install other third-party software which includes advertising.

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/i/istbar.asp

New Vulnerabilities found this Week

- **Samba Two Buffer Overflow Vulnerabilities**

“buffer overflows”

Two vulnerabilities have been reported in Samba, potentially allowing malicious people to compromise a vulnerability system.

1) The vulnerability is caused due to a boundary error when decoding base64 data during HTTP basic authentication. This can potentially be exploited to cause a buffer overflow.

2) The vulnerability is caused due to a boundary error in the code used to handle "mangling method = hash". This can potentially be exploited to cause a buffer overflow.

The default setting in Samba 3 and later is "mangling method = hash2". A default installation

of Samba 3 is therefore not vulnerable to issue 2.

Issue 1 affects Samba 3.0.2 to 3.0.4.
Issue 2 affects Samba 3.0.0 to 3.0.4 and Samba 2.2.9 and prior.

References : http://www.samba.org/samba/whatsnew/samba-3.0.5.html

- **PHPNuke Multiple Input Validation Vulnerabilities**

"multiple cross-site scripting and SQL injection vulnerabilities"

It is reported that PHPNuke is susceptible to multiple cross-site scripting and SQL injection vulnerabilities.

This can allow for theft of cookie-based authentication credentials and other attacks. Attackers may supply malicious parameters to manipulate the structure and logic of SQL queries.

These vulnerabilities were reported in version 7.3 of PHPNuke. Other versions may also be affected.

References : http://securityfocus.com/bid/10749/info/

- **Sun Solaris Volume Manager Denial Of Service Vulnerability**

"local denial of service vulnerability"

Reportedly the Sun Solaris Volume Manager is affected by a local denial of service vulnerability. This issue is due to a failure of the application to properly handle exceptional conditions.

An attacker might leverage this issue to cause a kernel panic in the affected computer, effectively denying service to legitimate users.

References : http://securityfocus.com/bid/10747/info/

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