netVigilance

ScoutNews Team **6 February 2004**

Issue #6

Weekly ScoutNews by netVigilance

Content this week

- **netVigilance News**
- **Top Security News Stories this Week**
- **New Vulnerabilities Tested in SecureScout**
- **Major New Vulnerabilities this Week**

---

netVigilance News

New and Improved: SecureScout SP 1.9.114.0 was shipped today with some significant new features:
1) Brand new Statistic feature in SP
2) Unicode – Support for multi-byte Character sets for enhanced translation – Arabic, Hebrew, Chinese, Japanese, Korean.
3) By Popular request - Scan with specific privileges for different jobs, allowing a job to run as guest, administrator, or any other user.
4) In the AdminClient there are new activity reports. These new reports are available by right clicking on the root or on a particular entity in the Account management window of the AdminClient.

- Activity reports / High scores
  This report shows all vulnerabilities found sorted by risk level then number of hits.
- Activity reports / High scores Top 50
  This report shows the first 50 vulnerabilities found sorted by number of hits
- Activity reports / High scores Top 50 (Commercial view)
  This report shows the first 50 vulnerabilities found sorted by number of hits.
  The difference with the previous reports is that the number of hits is replaced by the rank order.
- Search TC
  This report shows all the test cases that match a given string.
- Current Status
  This report shows the ranges and IP addresses allowed for a specified level and its children. The specified level can be the root, any level 1 or any level 2 or any level 3 entities.
- Activity Tracking
  This report shows for a specified period all activity performed for a specified level and its children. The specified level can be the root, any level 1 or any level 2 or any level 3 entities. The default proposed period is the current month.

Upcoming Seminar Notice: Seismo Technologies and netVigilance cordially invite you to the 'NORCAL Security Event of the Winter' in Santa Clara on March 8, San Francisco on March 9, And Sacramento on March 10 @ 6- 9 PM. To participate in an exciting evening with security experts, award winning products with solutions on topics such as Pre-Emptive Security and Information Security Management, please register today. Partner companies presenting solutions are **netVigilance** and Intellitactics. Please visit the Seismo Technologies website for registration information: www.seismo-

tech.com/register.html

Top Security News Stories this Week

- **Improved Service Packs for Server 2003 and XP to be Released This Year**

  In a further attempt to improve security, Microsoft has announced the release of Service Packs for Windows Server 2003 and Windows XP for the second half of this year. New shielding measures will allow enterprises using Windows Server 2003 to block access to their systems from companies whose security procedures are not up to standard. For those using Windows XP, Service Pack 2 will include a new security tool to stop viruses and worms by monitoring known vulnerabilities, removing the need for the IT department to immediately patch problems. Attachment blocking in Outlook and instant messaging is being improved to help prevent the spread of viruses, while memory protection is also being tweaked to reduce stack overruns, a common way of crashing PCs.

  http://www.vnunet.com/News/1152482
  By Iain Thomson - vnunet

- **IE Security Patch Nixes Some Apps. Modification Meant To Foil Net Scams Irks Some**

  Some Web developers are complaining that an Internet Explorer patch that's meant to foil Net scams is disabling some applications that didn't put a premium on security. Microsoft last week announced that a modification to its IE browser would stop the insecure practice of including sensitive information in links. The update, which was released Monday, had some Web site programmers up in arms Wednesday due to complaints from Web users that they could no longer log in to sites that secure entry through credentials included in the URL.

  http://www.msnbc.msn.com/id/4165095/
  By Robert Lemos – CNET

- **IT Losing Ground in Virus Battle**

  After years of success deploying more effective and smarter defenses, anti-virus researchers contacted last week in the wake of the MyDoom outbreak acknowledged for one of the first times that the battle may be getting away from them. The MyDoom virus, which hit Jan. 26 and infected several-hundred-thousand machines, is the fastest-spreading virus in the history of the Internet, experts said. At its peak late last week, MyDoom had infected one in every 12 pieces of e-mail, according to MessageLabs Inc., a New York-based e-mail security company. MyDoom also is the latest in a line of recent viruses that, while not particularly innovative, have been maddeningly effective.

  http://www.eweek.com/article2/0,4149,1489598,00.asp
  By Dennis Fisher – eWeek

- **Can Email Survive?**

  E-mail didn't need a year like this. Even without growing spam and virus problems, it was threatening to buckle under its own weight. E-mail users, particularly within businesses, have developed a fixation with the medium. For many, e-mail has all but replaced the telephone. With more mail, it becomes far easier to miss important messages and details. According to a recent study by Ferris Research, a San Francisco firm that follows the messaging market, users waste an hour each week

managing their e-mail. And only 9 minutes of that hour are related to spam and viruses. By the end of 2003, people were beginning to wonder whether e-mail was worth the hassle. In a recent report from the Pew Internet and American Life Project, 60 percent of those surveyed said that spam has reduced their e-mail use "in a significant way." Everyday consumers are not the only ones changing their habits. Even businesses as large as General Motors—which employs 340,000 people worldwide—are slowly moving away from e-mail. "We've seen a trend back toward voice mail," says Tony Scott, GM's CTO for information systems and services. "[People] know that urgent e-mail messages can get lost in all the spam."

http://www.pcmag.com/article2/0,4149,1464011,00.asp
Source: Cade Metz – PC Week

- **Web Applications Wide Open To Hackers**

According to security firm WebCohort's Application Defense Center, at least 92% of web applications are vulnerable to some form of attack. The results, based on tests of 250 applications over four years, shows cross-site scripting vulnerabilities accounting for 80% of weaknesses, SQL injections at 62%, and parameter tampering at 60%. The applications tested were on e-commerce, online banking, enterprise collaboration, and supply chain management websites. WebCohort also found that attackers could steal valuable data, shut down sites, and create legal liability while avoiding detection, despite widespread use of firewalls and intrusion detection systems. WebCohort chief executive Shlomo Kramer argues that tighter network security has pushed hackers to targeting the weaker web applications.

http://www.vnunet.com/News/1152521
By Robert Jaques – vnunet

- **Spyware Cures May Cause More Harm Than Good**

Users wishing to keep their computers clean of spyware, software that monitors computer use for fraud or to gather marketing data, are falling victim to so-called antispyware programs that come bundled with spyware. The Center for Democracy and Technology plans to file complaints with the Federal Trade Commission (FTC) against offending companies. Many antispyware companies have been unwilling to disclose their practices, while others put competitors' software on their lists of programs to remove in spyware scans. One program, SpyBan, has been discovered to download the Look2Me web-use monitor. SpyBan's website has gone offline after receiving questions about Look2Me from reporters. For a safe reliable spyware filter try Lavasoft Ad-Ware. Nice and clean.

http://news.com.com/2100-1032_3-5153485.html?tag=nefd_lede
By John Borland - CNET

New Vulnerabilities Tested in SecureScout

Seven new vulnerability Test Cases have been incorporated into the SecureScout database this week. Of course, these weekly updates are what keeps your network scanning tool one step in front of the hackers, inside or outside the organization.

- **14396 Cumulative Security Update for Internet Explorer**

This is a check for the cumulative update that includes the functionality of all the previously-released updates for Internet Explorer 5.01, Internet Explorer 5.5, and Internet Explorer 6.0. Additionally, it eliminates the following three newly-discovered vulnerabilities: A vulnerability

that involves the cross-domain security model of Internet Explorer. A vulnerability that involves performing a drag-and-drop operation with function pointers during dynamic HTML (DHTML) events in Internet Explorer. A vulnerability that involves the incorrect parsing of URLs that contain special characters.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1026
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1027
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1025
Microsoft Bulletin:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms04-004.asp

- **14397 .reg files associated with Regedit Vulnerability**

As all .reg files are associated with the Regedit.exe this makes the registry vulnerable to Trojan attacks.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0572
XForce: http://xforce.iss.net/xforce/xfdb/178
eEye: http://www.eeye.com/html/Products/Retina/RTHs/Registry/977.html
eEye: http://www.eeye.com/html/Products/Retina/RTHs/Registry/977.html

- **17833 phpGedView 2.61 PHP remote code injection vulnerability**

PHP remote code injection vulnerability in functions.php, authentication_index.php, and config_gedcom.php for PHPGEDVIEW 2.61 allows remote attackers to execute arbitrary PHP code by modifying the PGV_BASE_DIRECTORY parameter to reference a URL on a remote web server that contains the code.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0030
Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107340840209453&w=2
XForce: http://xforce.iss.net/xforce/xfdb/14159

- **17837 phpGedView 2.65 and prior PATH disclosure vulnerability**

PHPGEDVIEW 2.65 and prior allows malicious users to obtain the server-side scripts install PATH.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0066
Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107394912715478&w=2

- **17866 phpdig 1.6.5 and prior PHP remote code injection vulnerability**

  PHP remote code injection vulnerability in config.php for PhpDig 1.6.5 and earlier allows remote attackers to execute arbitrary PHP code by modifying the $relative_script_path parameter to reference a URL on a remote web server that contains the code.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0033
  Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107412194008671&w=2
  Web Site:
  http://www.phpdig.net/showthread.php?s=58bcc71c822830ec3bbdaae6d56846e0&threadid=393

- **17867 phpGedView 2.65.1 and prior Directory Traversal Vulnerability**

  Directory traversal vulnerability in editconfig_gedcom.php for phpGedView 2.65.1 and earlier allows remote attackers to read arbitrary files or execute arbitrary PHP programs on the server via .. (dot dot) sequences in the gedcom_config parameter. PHPGEDVIEW 2.65 and prior allows malicious users to access files on the server-side scripts harddisk.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0127
  Security Focus: http://www.securityfocus.com/archive/1/352355

- **17869 phpMyAdmin 2.5.5 and prior Directory Traversal Vulnerability**

  phpMyAdmin is a tool written in PHP intended to handle the administration of MySQL over the WWW. Directory traversal vulnerability in export.php in phpMyAdmin 2.5.5 and earlier allows remote attackers to read arbitrary files via .. (dot dot) sequences in the what parameter.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0129
  Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107582619125932&w=2
  Sourceforge: http://sourceforge.net/forum/forum.php?forum_id=350228

Major New Vulnerabilities this Week

PHP Code Injection Vulnerabilities in phpGedView 2.65.1 and Prior
PHP remote code injection vulnerability in the GEDCOM configuration script for phpGedView 2.65.1 and earlier allows remote attackers to execute arbitrary PHP code by modifying the PGV_BASE_DIRECTORY parameter to reference a URL on a remote web server that contains a malicious theme.php script. Credit for discovering this vulnerability goes to our very own Cedric Cochin.
For more information, see http://www.securityfocus.com/archive/1/352355
Source: Security Focus

Login.pho HTTP Request Does Not Contain Required Username/password Parameters

login.php in phpGedView 2.65 and earlier allows remote attackers to obtain sensitive information via an HTTP request to login.php that does not contain the required username or password parameters, which causes the information to be leaked in an error message.
For more information, see http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0130
Source: CVE Mitre

Check Point FireWall-1 HTTP Parsing Format String Vulnerabilities
Multiple vulnerabilities have been discovered in Check Point FireWall-1, which can be exploited by malicious people to compromise a vulnerable firewall.

The vulnerabilities are caused due to format string errors in the Application Intelligence component and the HTTP Security Server application proxy during parsing of HTTP traffic. This can be exploited to execute arbitrary code with SYSTEM or root privileges on a vulnerable firewall by sending specially crafted HTTP requests containing certain invalid data including format specifiers. Successful exploitation requires that HTTP Application Intelligence or the HTTP Security Server is enabled.
For more information, see http://www.secunia.com/advisories/10794/
http://news.com.com/2100-1002_3-5153635.html?part=rss&tag=feed&subj=news
Source: Secunia / CNET

GNU Radius Remote Denial of Service Vulnerability
Radius is a server for remote user authentication and accounting. Remote exploitation of a denial of service condition within GNU Radius can allow an attacker to crash the service. The problem specifically exists within the rad_print_request() routine defined in lib/logger.c. The denial of service condition is triggered upon the receipt of a single UDP packet that contains the attribute Acct-Status-Type. On line [0] within rad_print_request() the Acct-Status-Type attribute is accessed. On line [1] the Acct-Session-Id attribute is accessed. On line [2] the local pointer dval is set to point to the Acct-Status-Type attribute value. Because no value was specified for this attribute, dval is equal to NULL. The if-clause on line [3] fails causing line [4] to be executed. At this point due to the fact that there is no Acct-Session-Id attribute, sid_par is equal to NULL. This thereby makes the reference illegal and causes the application to crash.
For more information, see http://www.net-security.org/vuln.php?id=3236
Source: HelpNetSecurity

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.