netVigilance
assurance has arrived

# ScoutNews

*The weekly Security update from the makers of SecureScout*

2007 Issue # 19

May 18, 2007

**Table of Contents**

Product Focus

This Week in Review

Top Security News Stories this Week

New Vulnerabilities Tested in SecureScout

New Vulnerabilities found this Week

## Product Focus

**CodeRed Worm Scanner** – The CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

## This Week in Review

This week netVigilance Security Research has found 5 vulnerabilities in open source software:

2 high risk, 1 medium risk and 2 low risk. The vulnerabilities include SQL Injection, XSS (Cross site Scripting) and email injection.

The affected software include latest versions of popular open source software Jetbox Contents Management System, SonicBB and MyBB.

To see details and further information please see:
http://www.netvigilance.com/advisories

The price of a blunder. Check out a security survival guide. How do we act against phishing> Zango – a service or a threat?

Enjoy reading & 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

### ❖ TK Maxx security blunder will cost $8.3bn

45 million customers' cards at an estimated $186 each

TJX, the owner of TK Maxx, claimed in an earnings report today that the recent security blunder which exposed the credit card details of 45 million customers has cost the company $12 million.

The earnings report also refers to a similar charge expected in the next quarter.

"On 17 January TJX announced that it had suffered an unauthorised intrusion(s) into portions of its computer systems that process and store information related to customer transactions," the statement said.

"In the first quarter of fiscal 2008, the company recorded an after-tax charge of approximately $12 million, or $.03 per share, for costs incurred during the first quarter, which includes costs incurred to investigate and contain the intrusion, enhance computer security and systems, and communicate with customers, as well as technical, legal and other fees.

techcentral

Full Story :
http://www.techcentral.ie/corporate_it/TK_Maxx_security_blunder/view

### ❖ New Security Survival Guide: How To Layer A Solid Defense

As attacks on enterprise systems grow more sophisticated and diverse, companies need to rethink their defense strategies. In this special report, experts offer new and better ways to protect vital information resources.
A New Look at Layers
While emerging classes of tools may fend off attacks at multiple layers of a security strategy, there are pitfalls if the tools are not properly configured, managed or integrated with existing systems.

Layer 1: Perimeter Security
Layer 2: Host Security
Layer 3: Identity and Access Management
Layer 4: Network Access Control
Layer 5: Vulnerability Management
Layer Integration: Pulling It All Together

baseline

Full Story :
http://www.baselinemag.com/article2/0,1540,2132421,00.asp

### ❖ Co-operative 'coastguard' approach needed to beat 'phishing' menace

South African banks, Internet service providers (ISPs) and electronic messaging service specialists need to adopt a co-operative "coastguard" approach to overcome the threat posed by online fraud or "phishing".

"Co-operation and information sharing among major banks, will ensure a strong platform from which to fight this ongoing threat," said Mike Wright, CEO of Johannesburg-based international electronic secure e-mail and messaging specialist Striata.

"All of the parties involved have to present a united front to educate customers if we are to effectively combat ongoing efforts by criminals to defraud people by conning them into revealing their online banking details on copycat Web sites."

itweb

Full Story :
http://www.itweb.co.za/sections/techforum/2007/0705160807.asp?S=Electronic%20Billing%20and%20Marketing&A=EBI&O=FPIC

### ❖ Zango tries to get Spyware Doctor struck off

Adware maker Zango is suing PC Tools, makers of the popular Spyware Doctor software, in a dispute over the way the anti-spyware program flags and removes Zango's technology.
Representatives from both Zango and PC Tools confirmed that Zango had filed suit against the anti-spyware vendor. However they declined to provide details on the lawsuit except to say that it involved a dispute over the way Spyware Doctor rated Zango's software.

"We believe the proceedings are an attempt by Zango to influence our reclassification process," PC Tools said . "Prior to the lawsuit we were well into an in-depth review and reclassification of the latest versions of Zango products," PC Tools said. "We advised Zango of this imminent re-rating and we believe they have chosen to lodge these proceedings as a way to gain media attention of the review."

The Spyware Doctor Starter Edition that ships with Google Pack assigns Zango an "elevated" threat-level rating.

techworld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=8869&pagtype=samechan

# New Vulnerabilities Tested in SecureScout

### ❖ 16510 Microsoft DNS RPC Management Vulnerability (MS07-029/935966) (Remote File Checking)

A remote code execution vulnerability exists in the Domain Name System (DNS) Server Service in all supported server versions of Windows that could allow an attacker who

successfully exploited this vulnerability to take complete control of the affected system.

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

**References:**

Original advisory:
MS07-029
http://www.microsoft.com/technet/security/bulletin/ms07-029.mspx

Other references:
# MISC: http://blogs.technet.com/msrc/archive/2007/04/12/microsoft-security-advisory-935964-posted.aspx
# MISC: http://metasploit.com/svn/framework3/trunk/modules/exploits/windows/dcerpc/msdns_zonename.rb
# CONFIRM: http://www.microsoft.com/technet/security/advisory/935964.mspx
# CERT:TA07-103A
# URL:http://www.us-cert.gov/cas/techalerts/TA07-103A.html
# CERT-VN:VU#555920
# URL:http://www.kb.cert.org/vuls/id/555920
# BID:23470
# URL:http://www.securityfocus.com/bid/23470
# FRSIRT:ADV-2007-1366
# URL:http://www.frsirt.com/english/advisories/2007/1366
# SECTRACK:1017910
# URL:http://www.securitytracker.com/id?1017910
# SECUNIA:24871
# URL:http://secunia.com/advisories/24871
# XF:win-dns-rpc-bo(33629)
# URL:http://xforce.iss.net/xforce/xfdb/33629

**CVE Reference:** CVE-2007-1748

### ❖ 16508 Microsoft Internet Explorer Arbitrary File Rewrite Vulnerability (MS07-027/931768) (Remote File Checking)

A remote code execution vulnerability exists in a media service component that was never supported in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
MS07-027
http://www.microsoft.com/technet/security/bulletin/ms07-027.mspx

Other references:

# BID:23827
# URL:http://www.securityfocus.com/bid/23827
# FRSIRT:ADV-2007-1712
# URL:http://www.frsirt.com/english/advisories/2007/1712
# SECTRACK:1018019
# URL:http://www.securitytracker.com/id?1018019
# SECUNIA:23769
# URL:http://secunia.com/advisories/23769

**CVE Reference:** CVE-2007-2221

### ❖ 16504 Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability (MS07-027/931768) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
MS07-027
http://www.microsoft.com/technet/security/bulletin/ms07-027.mspx

Other references:
# FRSIRT:ADV-2007-1712
# URL:http://www.frsirt.com/english/advisories/2007/1712
# SECTRACK:1018019
# URL:http://www.securitytracker.com/id?1018019
# SECUNIA:23769
# URL:http://secunia.com/advisories/23769

**CVE Reference:** CVE-2007-0942

### ❖ 13528 MySQL SECURITY INVOKER Privilege Escalation Vulnerability

An issue has been reported in MySQL, which can be exploited by malicious users to gain escalated privileges.

The problem is that stored routines defined with SQL SECURITY INVOKER do not change back privileges when returning and can be invoked by users to gain escalated privileges.

The security issue has been reported in version 5.0.40.

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

**References:**

Original advisory:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html

Other references:
* MISC: http://bugs.mysql.com/bug.php?id=27337
* FRSIRT:ADV-2007-1804
* URL:http://www.frsirt.com/english/advisories/2007/1804

Product Homepage:
http://www.mysql.com/

**CVE Reference:** CVE-2007-2692

### ❖ 13527 MySQL Table renaming Privilege Escalation Vulnerability

An issue has been reported in MySQL, which can be exploited by malicious users to gain escalated privileges.

The problem is that it is possible for a user to rename a table without having DROP privileges.

The security issue has been reported in version 4.1 and 5.0.

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

**References:**

Original advisory:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html

Other references:
* MISC: http://bugs.mysql.com/bug.php?id=27515
* FRSIRT:ADV-2007-1804
* URL:http://www.frsirt.com/english/advisories/2007/1804

Product Homepage:
http://www.mysql.com/

**CVE Reference:** CVE-2007-2691

### ❖ 13526 MySQL IF Query Denial of Service Vulnerability

Neil Kettle has reported a vulnerability in MySQL, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when handling specially crafted IF queries, which can be exploited to crash the server.

The vulnerability is reported in versions prior to 5.0.40.

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

**References:**

Original advisory:
http://bugs.mysql.com/bug.php?id=27513
http://lists.mysql.com/commits/23685

Other references:
# GENTOO:GLSA-200705-11
# URL:http://security.gentoo.org/glsa/glsa-200705-11.xml
# BID:23911
# URL:http://www.securityfocus.com/bid/23911
# FRSIRT:ADV-2007-1731
# URL:http://www.frsirt.com/english/advisories/2007/1731
# SECUNIA:25196
# URL:http://secunia.com/advisories/25196
# SECUNIA:25188
# URL:http://secunia.com/advisories/25188

Product Homepage:
http://www.mysql.com/

**CVE Reference:** CVE-2007-2583

### ❖ 16503 Microsoft Exchange IMAP Literal Processing Vulnerability (MS07-026/931832) (Remote File Checking)

A denial of service vulnerability exists in Microsoft Exchange Server because of the way that it handles invalid IMAP requests. An attacker could exploit the vulnerability by sending a specially crafted IMAP command to a Microsoft Exchange Server configured as an IMAP server. An attacker successfully exploiting this vulnerability could cause the mail service to stop responding.

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

**References:**

Original advisory:
MS07-026
http://www.microsoft.com/technet/security/bulletin/ms07-026.mspx

Other references:
# BID:23810
# URL:http://www.securityfocus.com/bid/23810
# FRSIRT:ADV-2007-1711
# URL:http://www.frsirt.com/english/advisories/2007/1711
# SECTRACK:1018015

# URL:http://www.securitytracker.com/id?1018015
# SECUNIA:25183
# URL:http://secunia.com/advisories/25183

**CVE Reference:** CVE-2007-0221

### ❖ 16502 Microsoft Exchange MIME Decoding Vulnerability (MS07-026/931832) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Exchange Server because of the way that it decodes specially crafted e-mail messages. An attacker could exploit the vulnerability by sending a specially crafted e-mail to a Microsoft Exchange Server user account. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
MS07-026
http://www.microsoft.com/technet/security/bulletin/ms07-026.mspx

Other references:
# CERT-VN:VU#343145
# URL:http://www.kb.cert.org/vuls/id/343145
# BID:23809
# URL:http://www.securityfocus.com/bid/23809
# FRSIRT:ADV-2007-1711
# URL:http://www.frsirt.com/english/advisories/2007/1711
# SECTRACK:1018015
# URL:http://www.securitytracker.com/id?1018015
# SECUNIA:25183
# URL:http://secunia.com/advisories/25183

**CVE Reference:** CVE-2007-0213

### ❖ 16501 Microsoft Exchange Malformed iCal Vulnerability (MS07-026/931832) (Remote File Checking)

A denial of service vulnerability exists in Microsoft Exchange Server because of the way that it handles calendar content requests. An attacker could exploit the vulnerability by sending an e-mail message with specially crafted iCal file to a Microsoft Exchange Server user account. An attacker successfully exploiting this vulnerability could cause the mail service to stop responding.

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

**References:**

Original advisory:
MS07-026

http://www.microsoft.com/technet/security/bulletin/ms07-026.mspx

Other references:
# BID:23808
# URL:http://www.securityfocus.com/bid/23808
# FRSIRT:ADV-2007-1711
# URL:http://www.frsirt.com/english/advisories/2007/1711
# SECTRACK:1018015
# URL:http://www.securitytracker.com/id?1018015
# SECUNIA:25183
# URL:http://secunia.com/advisories/25183

**CVE Reference:** CVE-2007-0039

❖ **16499 Microsoft Exchange Outlook Web Access Script Injection Vulnerability (MS07-026/931832) (Remote File Checking)**

An information disclosure vulnerability exists in Microsoft Exchange in the way that Outlook Web Access (OWA) handles script-based attachments. An attached script could spoof content, disclose information, or take any action that the user could take within the context of the OWA session.

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

**References:**

Original advisory:
MS07-026
http://www.microsoft.com/technet/security/bulletin/ms07-026.mspx

Other references:
# CERT-VN:VU#124113
# URL:http://www.kb.cert.org/vuls/id/124113
# BID:23806
# URL:http://www.securityfocus.com/bid/23806
# FRSIRT:ADV-2007-1711
# URL:http://www.frsirt.com/english/advisories/2007/1711
# SECTRACK:1018015
# URL:http://www.securitytracker.com/id?1018015
# SECUNIA:25183
# URL:http://secunia.com/advisories/25183

**CVE Reference:** CVE-2007-0220

# New Vulnerabilities found this Week

**Norton Personal Firewall ISAlertDataCOM ActiveX Control Buffer Overflow**
"Execution of arbitrary code"

Will Dorman has reported a vulnerability in Norton Personal Firewall, which can be

exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the ISAlertDataCOM ActiveX control (ISLAlert.dll) when handling the "Set()" and "Get()" methods. This can be exploited to cause a stack-based buffer overflow via an overly long argument.

Successful exploitation allows execution of arbitrary code.

References:
http://securityresponse.symantec.com/avcenter/security/Content/2007.05.16.html
http://www.kb.cert.org/vuls/id/983953

### MySQL Two Privilege Escalation Security Issues

"Gain escalated privileges"

Two security issues have been reported in MySQL, which can be exploited by malicious users to gain escalated privileges.

1) The problem is that it is possible for a user to rename a table without having DROP privileges.

The security issue has been reported in version 4.1 and 5.0.

2) The problem is that stored routines defined with SQL SECURITY INVOKER do not change back privileges when returning and can be invoked by users to gain escalated privileges.

The security issue has been reported in version 5.0.40.

References:
http://bugs.mysql.com/bug.php?id=27515
http://bugs.mysql.com/bug.php?id=27337
http://descriptions.securescout.com/tc/13527
http://descriptions.securescout.com/tc/13528

### SonicBB SQL Injection and Cross-Site Scripting

"SQL injection attacks; cross-site scripting attacks"

Jesper Jurcenoks has discovered some vulnerabilities in SonicBB, which can be exploited by malicious people to conduct SQL injection attacks or cross-site scripting attacks.

1) Input passed to the "part" parameter in search.php or the "id" parameter in viewforum.php or members.php is not properly sanitised before being used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Successful exploitation of this vulnerability allows e.g. retrieving administrator usernames and password hashes, but requires that "magic_quotes_gpc" is disabled.

### 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