

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

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Apache Chunked Encoding buffer overflow.

Download Here:

<http://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Retailers under attack. Sony breached again. Critical fixes from Microsoft. Largest ID theft takedown in US history.

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

• Hacker attacks against retailers up 43 percent

Hacks targeting the retail sector have increased 43 percent since last year, largely due to an increase in SQL injection and the use of exploit toolkits, according to researchers at Dell SecureWorks.

During the first nine months of 2011, Dell SecureWorks blocked an average of 91,500 attacks per retailer, compared to 63,651 during the final nine months of 2010. The rise is primarily due to an increase in SQL injection assaults against servers, as well as attacks stemming from web-based exploit kits, Ben Feinstein, director of operations and analysis with the Dell SecureWorks Counter Threat Unit, told SCMagazineUS.com on Tuesday.

Other verticals have also experienced an increase in attacks, though not to the same degree as the retail sector, he said. Merchants are being more heavily targeted than those within other sectors, likely because they maintain vast amounts of information that attackers want, and often have less stringent security controls. SC Magazine

Full Story :

http://www.scmagazineus.com/hacker-attacks-against-retailers-up-43-percent/article/214125/?utm_source=feedburn

• Another PlayStation Network breach stings Sony customers

Sony on Wednesday said hackers have again accessed its network, this time compromising the accounts of some 93,000 customers.

But it appears the electronics giant was able to quickly detect the attack, which affected some 60,000 PlayStation Network (PSN) and Sony Entertainment Network gamers, and 33,000 Sony Online Entertainment (SOE) users.

In a statement, Sony said the intruders used "very large sets of sign-in IDs and passwords" in an attempt to verify user accounts, a trial-and-error method known as brute force. To do this, the hackers appeared to use login data they stole "from other companies, sites or sources," according to Sony. SC Magazine

Full Story :

http://www.scmagazineus.com/another-playstation-network-breach-stings-sony-customers/article/214179/?utm_source=

• Internet Explorer fixes get top billing in Microsoft update

Microsoft on Tuesday released eight fixes to address 23 vulnerabilities that lie across its software and operating system components.

Most notable is bulletin MS11-081, a "critical" patch that closes eight privately reported holes in Internet Explorer (IE) and affects all supported versions, including IE 9. Some of the vulnerabilities can be exploited simply by a user visiting a malicious website.

The only other critical fix is MS11-078, which repairs a privately reported vulnerability in .NET Framework and Silverlight. SC Magazine

Full Story :

http://www.scmagazineus.com/internet-explorer-fixes-get-top-billing-in-microsoft-update/article/214143/?utm_source=

• More than 100 charged in ID theft ring

In what is being termed the largest identity theft takedown in U.S. history, 111 individuals have been charged for their involvement in an organized crime operation responsible for more than \$13 million in losses over a 16-month period.

The defendants, 86 of whom are currently in custody, are members of five credit card fraud and identity theft groups, based in Queens County, N.Y., with ties to Europe, Asia, Africa and the Middle East, prosecutors said in a Friday statement. Twenty-five suspects are still being sought by law enforcement.

"This is by far the largest - and certainly among the most sophisticated - identity theft/credit card fraud cases that law enforcement has come across," Queens County District Attorney Richard Brown said. SC Magazine

Full Story :

http://www.scmagazineus.com/more-than-100-charged-in-id-theft-ring/article/214024/?utm_source=feedburner&utm=

New Vulnerabilities Tested in SecureScout

• 13825 MySQL Infinite loop via multiple invocations Denial of Service Vulnerability

MySQL 5.1 before 5.1.51 and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (infinite loop) via multiple invocations of a (1) prepared statement or (2) stored procedure that creates a query with nested JOIN statements.

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

References:

* CONFIRM:

<http://bugs.mysql.com/bug.php?id=53544>

* CONFIRM:

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-51.html>

* CONFIRM:

<http://dev.mysql.com/doc/refman/5.5/en/news-5-5-6.html>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=640861

* MANDRIVA: MDVSA-2010:222

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:222>

* MANDRIVA: MDVSA-2010:223

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:223>

* REDHAT: RHSA-2010:0825

<http://www.redhat.com/support/errata/RHSA-2010-0825.html>

* REDHAT: RHSA-2011:0164

<http://www.redhat.com/support/errata/RHSA-2011-0164.html>

* UBUNTU: USN-1017-1

<http://www.ubuntu.com/usn/USN-1017-1>

* BID: 43676

<http://www.securityfocus.com/bid/43676>

* SECUNIA: 42936

<http://secunia.com/advisories/42936>

* VUPEN: ADV-2011-0170

<http://www.vupen.com/english/advisories/2011/0170>

* XF: mysql-invocations-dos(64839)

<http://xforce.iss.net/xforce/xfdb/64839>

CVE Reference:

CVE-2010-3839 (cve.mitre.org, nvd.nist.gov)

• 19493 Apache HTTP Server Denial of Service Vulnerabilities

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

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

References:

* EXPLOIT-DB: 17696

<http://www.exploit-db.com/exploits/17696>

* FULLDISC: 20110820 Apache Killer

<http://seclists.org/fulldisclosure/2011/Aug/175>

* FULLDISC: 20110824 Re: Apache Killer

<http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0285.html>

* MLIST: [announce] 20110824 Advisory: Range header DoS vulnerability Apache HTTPD 1.3/2.x
\\(CVE-2011-3192)

http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3c20110824161640.122D387DD@minotaur.a

* CONFIRM:

<http://www.gossamer-threads.com/lists/apache/dev/401638>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=732928

* CONFIRM:

https://issues.apache.org/bugzilla/show_bug.cgi?id=51714

* SECTRACK: 1025960

<http://securitytracker.com/id?1025960>

* SECUNIA: 45606

<http://secunia.com/advisories/45606>

* BID: 49303

<http://www.securityfocus.com/bid/49303>

CVE Reference:

CVE-2011-3192 (cve.mitre.org, nvd.nist.gov)

• 19516 Microsoft Hyper-V VMBus Denial of Service Vulnerability (MS11-047/2525835) (Remote File Checking)

Microsoft Hyper-V is prone to a local denial-of-service vulnerability.

Using a guest system, a local attacker can exploit this issue to force the Hyper-V server to become unresponsive, denying service to legitimate users. The denial-of-service conditions would also affect other guest operating systems.

The vulnerability could allow denial of service if a specially crafted packet is sent to the VMBus by an authenticated user in one of the guest virtual machines hosted by the Hyper-V server. An attacker must have valid logon credentials and be able to send specially crafted content from a guest virtual machine to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

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

References:

* MS: MS11-047

<http://www.microsoft.com/technet/security/Bulletin/MS11-047.mspx>

* BID: 48179

<http://www.securityfocus.com/bid/48179>

* OVAL: oval:org.mitre.oval:def:12650

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12650>

* SECTRACK: 1025644

<http://www.securitytracker.com/id?1025644>

CVE Reference:

CVE-2011-1872 (cve.mitre.org, nvd.nist.gov)

• 19517 Microsoft Windows SMB Server Remote Denial of Service Vulnerability (MS11-048/2536275) (Remote File Checking)

Microsoft Windows is prone to a remote denial-of-service vulnerability.

An attacker can exploit this issue to crash the SMB server, denying service to legitimate users.

The vulnerability could allow denial of service if an attacker created a specially crafted SMB packet and sent the packet to an affected system. Firewall best practices and standard default firewall configurations can help protect networks from attacks originating outside the enterprise perimeter that would attempt to exploit this vulnerability.

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

References:

* MS: MS11-048

<http://www.microsoft.com/technet/security/Bulletin/MS11-048.mspx>

* OVAL: oval:org.mitre.oval:def:12654

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12654>

CVE Reference:

CVE-2011-1267 (cve.mitre.org, nvd.nist.gov)

• 19519 Microsoft Active Directory Certificate Services Web Enrollment Cross-Site Scripting Vulnerability (MS11-051/2518295) (Remote File Checking)

Microsoft Active Directory Certificate Services are prone to a cross-site scripting vulnerability because the Web Enrollment component fails to properly sanitize user-supplied input.

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal potentially sensitive information and launch other attacks.

The vulnerability is a cross-site scripting (XSS) vulnerability that could allow elevation of privilege, enabling an attacker to execute arbitrary commands on the site in the context of the target user. An attacker who successfully exploited this vulnerability would need to send a specially crafted link and convince a user to click the link. In all cases, however, an attacker would have no way to force a user to visit the Web site. Instead, an attacker would have to persuade a user to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes the user to the vulnerable Web site.

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

References:

* MS: MS11-051

<http://www.microsoft.com/technet/security/Bulletin/MS11-051.mspx>

* OVAL: oval:org.mitre.oval:def:12749

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12749>

* BID: 48175

<http://www.securityfocus.com/bid/48175/discuss>

CVE Reference:

CVE-2011-1264 (cve.mitre.org, nvd.nist.gov)

• 19520 Microsoft Internet Explorer VML Memory Corruption Remote Code Execution Vulnerability (MS11-052/2544521) (Remote File Checking)

Microsoft Internet Explorer is prone to a remote code-execution vulnerability due to a memory-corruption error.

Attackers can exploit this issue by enticing an unsuspecting user to view a specially crafted webpage.

Successful exploits may allow attackers to execute arbitrary code with the privileges of the user running the affected application. Failed exploit attempts will likely result in a denial-of-service condition.

The vulnerability could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

The security update addresses the vulnerability by modifying the way that Internet Explorer handles objects in memory.

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

References:

- * MS: MS11-052
<http://www.microsoft.com/technet/security/Bulletin/MS11-052.msp>
- * OVAL: oval:org.mitre.oval:def:12593
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12593>

CVE Reference:

CVE-2011-1266 (cve.mitre.org, nvd.nist.gov)

• **19521 Microsoft Windows Bluetooth Stack 'bthport.sys' Driver Remote Code Execution Vulnerability (MS11-053/2566220) (Remote File Checking)**

Microsoft Windows is prone to a remote code-execution vulnerability.

The vulnerability could allow remote code execution if an attacker sent a series of specially crafted Bluetooth packets to an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability only affects systems with Bluetooth capability.

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

References:

- * MS: MS11-053
<http://www.microsoft.com/technet/security/Bulletin/MS11-053.msp>
- * CERT: TA11-193A
<http://www.us-cert.gov/cas/techalerts/TA11-193A.html>
- * OVAL: oval:org.mitre.oval:def:12094
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12094>
- * BID: 48617
<http://www.securityfocus.com/bid/48617/info>

CVE Reference:

CVE-2011-1265 (cve.mitre.org, nvd.nist.gov)

• **19522 Microsoft Windows CSRSS 'AllocConsole()' Local Privilege Escalation Vulnerability (MS11-056/2507938) (Remote File Checking)**

Microsoft Windows is prone to a local privilege-escalation vulnerability.

An attacker can exploit this issue to execute arbitrary code with SYSTEM-level privileges. The vulnerabilities could allow elevation of privilege if an attacker logs on to a user's system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit the vulnerabilities.

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

References:

- * MS: MS11-056
<http://www.microsoft.com/technet/security/Bulletin/MS11-056.msp>
- * CERT: TA11-193A
<http://www.us-cert.gov/cas/techalerts/TA11-193A.html>
- * OVAL: oval:org.mitre.oval:def:12602
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12602>
- * BID: 48588
<http://www.securityfocus.com/bid/48588/info>

CVE Reference:

CVE-2011-1281 (cve.mitre.org, nvd.nist.gov)

• **19523 Microsoft Windows CSRSS 'SrvSetConsoleLocalEUDC()' Local Privilege Escalation Vulnerability (MS11-056/2507938) (Remote File Checking)**

Microsoft Windows is prone to a local privilege-escalation vulnerability.

An attacker can exploit this issue to execute arbitrary code with SYSTEM-level privileges. Successfully exploiting this issue will result in the complete compromise of affected computers. Failed exploit attempts will result in a denial-of-service condition.

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

References:

- * MS: MS11-056
<http://www.microsoft.com/technet/security/Bulletin/MS11-056.msp>
- * CERT: TA11-193A
<http://www.us-cert.gov/cas/techalerts/TA11-193A.html>
- * OVAL: oval:org.mitre.oval:def:12402
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12402>

CVE Reference:

CVE-2011-1282 (cve.mitre.org, nvd.nist.gov)

• 19524 Microsoft Windows CSRSS 'SrvSetConsoleNumberOfCommands()' Local Privilege Escalation Vulnerability (MS11-056/2507938) (Remote File Checking)

Microsoft Windows is prone to a local privilege-escalation vulnerability.

A local privilege-escalation vulnerability affects the Client/Server Runtime Subsystem (CSRSS) due to user-supplied input being used as an index for an array. A local attacker can exploit this issue to elevate their privileges to SYSTEM level. This will facilitate a complete compromise of the affected computer.

An attacker can exploit this issue to execute arbitrary code with SYSTEM-level privileges. Successfully exploiting this issue will result in the complete compromise of affected computers.

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

References:

- * MS: MS11-056
<http://www.microsoft.com/technet/security/Bulletin/MS11-056.msp>
- * CERT: TA11-193A
<http://www.us-cert.gov/cas/techalerts/TA11-193A.html>
- * OVAL: oval:org.mitre.oval:def:12362
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12362>
- * BID: 48604
<http://www.securityfocus.com/bid/48604>

CVE Reference:

CVE-2011-1283 (cve.mitre.org, nvd.nist.gov)

• 19525 Microsoft Windows CSRSS 'SrvWriteConsoleOutput()' Local Privilege Escalation Vulnerability (MS11-056/2507938) (Remote File Checking)

Microsoft Windows is prone to a local privilege-escalation vulnerability.

A local privilege-escalation vulnerability affects the Client/Server Runtime Subsystem (CSRSS) due to an integer-overflow. A local attacker can exploit this issue to elevate their privileges to SYSTEM level. This will facilitate a complete compromise of the affected computer.

An attacker can exploit this issue to execute arbitrary code with SYSTEM-level privileges. Successfully exploiting this issue will result in the complete compromise of affected computers.

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

References:

- * MS: MS11-056
<http://www.microsoft.com/technet/security/Bulletin/MS11-056.msp>
- * CERT: TA11-193A
<http://www.us-cert.gov/cas/techalerts/TA11-193A.html>
- * OVAL: oval:org.mitre.oval:def:12734
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12734>
- * BID: 48606
<http://www.securityfocus.com/bid/48606>

CVE Reference:

CVE-2011-1284 (cve.mitre.org, nvd.nist.gov)

• 19526 Microsoft Windows CSRSS 'SrvWriteConsoleOutputString()' Local Privilege Escalation Vulnerability (MS11-056/2507938) (Remote File Checking)

Microsoft Windows is prone to a local privilege-escalation vulnerability.

A local privilege-escalation vulnerability affects the Client/Server Runtime Subsystem (CSRSS) due to an integer-overflow. A local attacker can exploit this issue to elevate their privileges to SYSTEM level. This will facilitate a complete compromise of the affected computer.

An attacker can exploit this issue to execute arbitrary code with SYSTEM-level privileges. Successfully exploiting this issue will result in the complete compromise of affected computers.

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

References:

* MS: MS11-056

<http://www.microsoft.com/technet/security/Bulletin/MS11-056.msp>

* CERT: TA11-193A

<http://www.us-cert.gov/cas/techalerts/TA11-193A.html>

* BID: 48605

<http://www.securityfocus.com/bid/48605>

* OSVDB: 73795

<http://osvdb.org/73795>

* OVAL: oval:org.mitre.oval:def:12889

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12889>

CVE Reference:

CVE-2011-1870 (cve.mitre.org, nvd.nist.gov)

• 19527 PHP set_magic_quotes_runtime function SQL injection Vulnerability

The set_magic_quotes_runtime function in PHP 5.3.2 and 5.3.3, when the MySQLi extension is used, does not properly interact with use of the mysqli_fetch_assoc function, which might make it easier for context-dependent attackers to conduct SQL injection attacks via crafted input that had been properly handled in earlier PHP versions.

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

References:

* CONFIRM:

<http://bugs.php.net/52221>

* CONFIRM:

<http://www.php.net/ChangeLog-5.php>

* BID: 46056

<http://www.securityfocus.com/bid/46056>

* OVAL: oval:org.mitre.oval:def:12620

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12620>

* XF: php-setmagicquotesruntime-sql-injection(64964)

<http://xforce.iss.net/xfdb/64964>

CVE Reference:

CVE-2010-4700 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1999 Microsoft CVSS 2.0 Score = 9.3

Microsoft Internet Explorer 8 does not properly allocate and access memory, which allows remote attackers to execute arbitrary code via vectors involving a "dereferenced memory address," aka "Select Element Remote Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference: [CVE-2011-1999](#)

• **CVE-2011-2000 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "Body Element Remote Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference: [CVE-2011-2000](#)

• **CVE-2011-1997 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "OnLoad Event Remote Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference: [CVE-2011-1997](#)

• **CVE-2011-1998 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that was not properly initialized, aka "Jscript9.dll Remote Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference: [CVE-2011-1998](#)

• **CVE-2011-1996 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 through 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "Option Element Remote Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference: [CVE-2011-1996](#)

• **CVE-2011-1995 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that was not properly initialized, aka "OLEAuto32.dll Remote Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-081>

CVE Reference: [CVE-2011-1995](#)

• **CVE-2011-1969 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, Update 1, Update 2, and SP1 provides the MicrosoftClient.jar file containing a signed Java applet, which allows remote attackers to execute arbitrary code on client machines via unspecified vectors, aka "Poisoned Cup of Code Execution Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-079>

CVE Reference: [CVE-2011-1969](#)

• **CVE-2011-1253 Microsoft CVSS 2.0 Score = 9.3**

Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.5.1, and 4, and Silverlight 4 before 4.0.60831, does not properly restrict inheritance, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (aka XBAP), (2) a crafted ASP.NET application, (3) a crafted .NET Framework application, or (4) a crafted Silverlight application, aka ".NET Framework Class Inheritance Vulnerability."

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

References:

MS: <http://technet.microsoft.com/en-us/security/bulletin/MS11-078>

CVE Reference: [CVE-2011-1253](#)

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