

## 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://www.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

## This Week in Review

PCI compliance seen as necessary and positive for overall security. One of every five spam comes from the US. Bank warns of possible data breach via hacked laptop. Advice on how to avoid scams.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • Views regarding PCI compliance are mostly positive

Most IT security practitioners believe the Payment Card Industry Data Security Standard (PCI DSS) is necessary for protecting cardholder data and think their organization is more secure today because of it, according to a survey released Wednesday by Cisco. The survey of 500 IT security decision makers across health care, finance, retail, education and government sectors found that most organizations have taken significant steps to become compliant with the standard. A majority of survey respondents were "very confident" they could pass an assessment today.

When asked about their sentiments regarding PCI compliance, 36 percent of respondents said it is not only necessary for protecting cardholder data, but that they don't mind dealing with it. Another 52 percent called the standard "burdensome but necessary." SC Magazine

Full Story :

[http://www.scmagazineus.com/views-regarding-pci-compliance-are-mostly-positive/article/194130/?utm\\_source=feed](http://www.scmagazineus.com/views-regarding-pci-compliance-are-mostly-positive/article/194130/?utm_source=feed)

### • Report: U.S. leads world in spam output

The U.S. is the spam leader across the world, responsible for one out of every five junk messages sent, according to a report out today from Sophos.

The security vendor's fourth-quarter "Dirty Dozen" report of spam-relaying countries found that the United States upped its percentage of global spam from the third quarter and now accounts for 18.83 percent of all junk e-mails.

That percentage is almost three times higher than second-place India, which is responsible for deploying 6.88 percent of all spam across the globe, according to Sophos. Other countries named on the Dirty Dozen list include Brazil, Russia, the U.K., and France. Cnet Security

Full Story :

[http://news.cnet.com/8301-1009\\_3-20028151-83.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1009_3-20028151-83.html?part=rss&subj=news&tag=2547-1_3-0-20)

### • Hacked laptops lead banks to warn of data breaches

IDG News Service - Recent data breaches at two banks underscore what's becoming a gnarly problem for companies that handle sensitive information: When does a hacked PC become a data breach?

Sovereign Bank noticed its problem on Oct. 15, when staffers discovered a computer on their network connecting to an unusual IP address. After investigating, they found a keylogger program on a company laptop. Sovereign isn't releasing many details on the incident, but in December it notified 50 customers nationwide that their data may have been compromised. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9204819/Hacked\\_laptops\\_lead\\_banks\\_to\\_warn\\_of\\_data\\_breaches?source=](http://www.computerworld.com/s/article/9204819/Hacked_laptops_lead_banks_to_warn_of_data_breaches?source=)

### • How to avoid growing number of Internet scams

Hard times seem to make people more vulnerable to ploys designed to separate them from their money and personal information. At least half of BBB Online's list of the Top 10 scams of 2010 occur in whole or in part over the Internet.

The best way to avoid being victimized by scammers is to be very careful about who you trust. Here are five ways to protect yourself from attacks on your bank accounts and private data.

Don't pay upfront Cnet Security

Full Story :

[http://news.cnet.com/8301-13880\\_3-20028047-68.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-13880_3-20028047-68.html?part=rss&subj=news&tag=2547-1_3-0-20)

## New Vulnerabilities Tested in SecureScout

### • 18721 Movie Maker and Producer Buffer Overflow Vulnerability (MS10-016/975561) (Remote File Checking)

A remote code execution vulnerability exists in the way that Windows Movie Maker and Microsoft Producer 2003 handle specially crafted project files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

#### References:

\* BID: 38515

<http://www.securityfocus.com/bid/38515>

\* VUPEN: VUPEN/ADV-2010-0565

<http://www.vupen.com/english/advisories/2010/0565>

\* SECTRACK: 1023697

<http://securitytracker.com/alerts/2010/Mar/1023697.html>

\* MS: MS10-016

<http://www.microsoft.com/technet/security/bulletin/ms10-016.msp>

\* CERT: TA10-068A

<http://www.us-cert.gov/cas/techalerts/TA10-068A.html>

\* OVAL: oval:org.mitre.oval:def:8595

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8595>

#### CVE Reference:

CVE-2010-0265 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 18849 COM Validation Vulnerability (Microsoft Office) (MS10-036/983235) (Remote File Checking)

A remote code execution vulnerability exists in the way that affected Microsoft Office software validates COM object instantiation. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

This TC checks for the vulnerability specifically in Microsoft Office.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-1393  
<http://www.vupen.com/english/advisories/2010/1393>
- \* SECTRACK: 1024073  
<http://securitytracker.com/alerts/2010/Jun/1024073.html>
- \* MS: MS10-036  
<http://www.microsoft.com/technet/security/bulletin/ms10-036.msp>
- \* MS: MS10-083  
<http://www.microsoft.com/technet/security/Bulletin/MS10-083.msp>
- \* CERT: TA10-159B  
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- \* BID: 40574  
<http://www.securityfocus.com/bid/40574>
- \* OVAL: oval:org.mitre.oval:def:7286  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7286>
- \* SECTRACK: 1024555  
<http://www.securitytracker.com/id?1024555>

#### CVE Reference:

CVE-2010-1263 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19134 DSN Overflow Vulnerability (MS11-002/2451910) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Data Access Components validates third-party API usage. This vulnerability could allow code execution if a user visited a specially crafted Web page. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

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

#### References:

- \* VUPEN: VUPEN/ADV-2011-0075  
<http://www.vupen.com/english/advisories/2011/0075>
- \* SECTRACK: 1024947  
<http://securitytracker.com/id?1024947>
- \* BID: 45695  
<http://www.securityfocus.com/bid/45695>
- \* MS: MS11-002  
<http://www.microsoft.com/technet/security/Bulletin/MS11-002.msp>

#### CVE Reference:

CVE-2011-0026 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19135 ADO Record Memory Vulnerability (MS11-002/2451910) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Data Access Components validates memory allocation. This vulnerability could allow code execution if a user visited a specially crafted Web page. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

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

#### References:

- \* VUPEN: VUPEN/ADV-2011-0075  
<http://www.vupen.com/english/advisories/2011/0075>

\* SECTRACK: 1024947  
<http://securitytracker.com/id?1024947>  
\* BID: 45698  
<http://www.securityfocus.com/bid/45698>  
\* MS: MS11-002  
<http://www.microsoft.com/technet/security/Bulletin/MS11-002.mspx>

**CVE Reference:**

CVE-2011-0027 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19136 Backup Manager Insecure Library Loading Vulnerability (MS11-001/2478935) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the Microsoft Windows Backup Manager handles the loading of DLL files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

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

**References:**

\* VUPEN: VUPEN/ADV-2011-0074  
<http://www.vupen.com/english/advisories/2011/0074>  
\* SECTRACK: 1024948  
<http://securitytracker.com/id?1024948>  
\* BID: 42763  
<http://www.securityfocus.com/bid/42763>  
\* EXPLOIT-DB: 14751  
<http://www.exploit-db.com/exploits/14751/>  
\* MS: MS11-001  
<http://www.microsoft.com/technet/security/Bulletin/MS11-001.mspx>

**CVE Reference:**

CVE-2010-3145 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19137 BranchCache Insecure Library Loading Vulnerability (MS10-095/2385678) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Windows opens specific files on platforms that do not support the BranchCache functionality. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

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

**References:**

\* MS: MS10-095  
<http://www.microsoft.com/technet/security/Bulletin/MS10-095.mspx>  
\* CERT: TA10-348A  
<http://www.us-cert.gov/cas/techalerts/TA10-348A.html>  
\* BID: 45295  
<http://www.securityfocus.com/bid/45295>  
\* OSVDB: 69816  
<http://osvdb.org/69816>  
\* SECTRACK: 1024877  
<http://www.securitytracker.com/id?1024877>  
\* SECUNIA: 42609  
<http://secunia.com/advisories/42609>  
\* VUPEN: ADV-2010-3218  
<http://www.vupen.com/english/advisories/2010/3218>

**CVE Reference:**

CVE-2010-3966 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19138 COM Validation Vulnerability (Microsoft Office Excel) (MS10-036/983235) (Remote File Checking)**

A remote code execution vulnerability exists in the way that affected Microsoft Office software validates COM object instantiation. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

This TC checks for the vulnerability specifically in Microsoft Office Excel.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-1393  
<http://www.vupen.com/english/advisories/2010/1393>
- \* SECTRACK: 1024073  
<http://securitytracker.com/alerts/2010/Jun/1024073.html>
- \* MS: MS10-036  
<http://www.microsoft.com/technet/security/bulletin/ms10-036.msp>
- \* MS: MS10-083  
<http://www.microsoft.com/technet/security/Bulletin/MS10-083.msp>
- \* CERT: TA10-159B  
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- \* BID: 40574  
<http://www.securityfocus.com/bid/40574>
- \* OVAL: oval:org.mitre.oval:def:7286  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7286>
- \* SECTRACK: 1024555  
<http://www.securitytracker.com/id?1024555>

#### CVE Reference:

CVE-2010-1263 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19139 COM Validation Vulnerability (Microsoft Office PowerPoint) (MS10-036/983235) (Remote File Checking)

A remote code execution vulnerability exists in the way that affected Microsoft Office software validates COM object instantiation. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

This TC checks for the vulnerability specifically in Microsoft Office PowerPoint.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-1393  
<http://www.vupen.com/english/advisories/2010/1393>
- \* SECTRACK: 1024073  
<http://securitytracker.com/alerts/2010/Jun/1024073.html>
- \* MS: MS10-036  
<http://www.microsoft.com/technet/security/bulletin/ms10-036.msp>
- \* MS: MS10-083  
<http://www.microsoft.com/technet/security/Bulletin/MS10-083.msp>
- \* CERT: TA10-159B  
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- \* BID: 40574  
<http://www.securityfocus.com/bid/40574>
- \* OVAL: oval:org.mitre.oval:def:7286  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7286>
- \* SECTRACK: 1024555  
<http://www.securitytracker.com/id?1024555>

#### CVE Reference:

CVE-2010-1263 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19140 COM Validation Vulnerability (Microsoft Office Publisher) (MS10-036/983235) (Remote File Checking)

A remote code execution vulnerability exists in the way that affected Microsoft Office software validates COM object instantiation. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

This TC checks for the vulnerability specifically in Microsoft Office Publisher.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-1393  
<http://www.vupen.com/english/advisories/2010/1393>
- \* SECTRACK: 1024073  
<http://securitytracker.com/alerts/2010/Jun/1024073.html>
- \* MS: MS10-036  
<http://www.microsoft.com/technet/security/bulletin/ms10-036.msp>
- \* MS: MS10-083  
<http://www.microsoft.com/technet/security/Bulletin/MS10-083.msp>
- \* CERT: TA10-159B  
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- \* BID: 40574  
<http://www.securityfocus.com/bid/40574>
- \* OVAL: oval:org.mitre.oval:def:7286  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7286>
- \* SECTRACK: 1024555  
<http://www.securitytracker.com/id?1024555>

#### CVE Reference:

CVE-2010-1263 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19141 COM Validation Vulnerability (Microsoft Office Visio) (MS10-036/983235) (Remote File Checking)

A remote code execution vulnerability exists in the way that affected Microsoft Office software validates COM object instantiation. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

This TC checks for the vulnerability specifically in Microsoft Office Visio.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-1393  
<http://www.vupen.com/english/advisories/2010/1393>
- \* SECTRACK: 1024073  
<http://securitytracker.com/alerts/2010/Jun/1024073.html>
- \* MS: MS10-036  
<http://www.microsoft.com/technet/security/bulletin/ms10-036.msp>
- \* MS: MS10-083  
<http://www.microsoft.com/technet/security/Bulletin/MS10-083.msp>
- \* CERT: TA10-159B  
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- \* BID: 40574  
<http://www.securityfocus.com/bid/40574>
- \* OVAL: oval:org.mitre.oval:def:7286  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7286>
- \* SECTRACK: 1024555  
<http://www.securitytracker.com/id?1024555>

#### CVE Reference:

CVE-2010-1263 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

• **CVE-2011-0026 Microsoft CVSS 2.0 Score = 9.3**

Integer signedness error in the SQLConnectW function in an ODBC API (odbc32.dll) in Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, allows remote attackers to execute arbitrary code via a long string in the Data Source Name (DSN) and a crafted szDSN argument, which bypasses a signed comparison and leads to a buffer overflow, aka "DSN Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-002.msp>

**CVE Reference:** [CVE-2011-0026](#)

• **CVE-2011-0027 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Data Access Components (MDAC) 2.8 SP1 and SP2, and Windows Data Access Components (WDAC) 6.0, does not properly validate memory allocation for internal data structures, which allows remote attackers to execute arbitrary code, possibly via a large CacheSize property that triggers an integer wrap and a buffer overflow, aka "ADO Record Memory Vulnerability." NOTE: this might be a duplicate of CVE-2010-1117 or CVE-2010-1118.

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-002.msp>

**CVE Reference:** [CVE-2011-0027](#)

• **CVE-2010-3676 MySQL CVSS 2.0 Score = 4.0**

storage/innobase/dict/dict0crea.c in mysqld in MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (assertion failure) by modifying the (1) innodb\_file\_format or (2) innodb\_file\_per\_table configuration parameters for the InnoDB storage engine, then executing a DDL statement.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=628660](https://bugzilla.redhat.com/show_bug.cgi?id=628660)

MLIST: <http://www.openwall.com/lists/oss-security/2010/09/28/10>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html>

CONFIRM: <http://bugs.mysql.com/bug.php?id=55039>

**CVE Reference:** [CVE-2010-3676](#)

• **CVE-2010-3677 MySQL CVSS 2.0 Score = 4.0**

MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via a join query that uses a table with a unique SET column.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=628040](https://bugzilla.redhat.com/show_bug.cgi?id=628040)

MLIST: <http://www.openwall.com/lists/oss-security/2010/09/28/10>

SUSE: <http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00006.html>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html>

CONFIRM: <http://dev.mysql.com/doc/refman/5.0/en/news-5-0-92.html>

MISC: <http://bugs.mysql.com/bug.php?id=54575>

**CVE Reference:** [CVE-2010-3677](#)

• **CVE-2010-3678 MySQL CVSS 2.0 Score = 4.0**

MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (crash) via (1) IN or (2) CASE operations with NULL arguments that are explicitly specified or indirectly provided by the WITH ROLLUP modifier.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=628172](https://bugzilla.redhat.com/show_bug.cgi?id=628172)

MLIST: <http://www.openwall.com/lists/oss-security/2010/09/28/10>

CONFIRM: <http://bugs.mysql.com/bug.php?id=54477>

SUSE: <http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00006.html>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html>

**CVE Reference:** [CVE-2010-3678](#)

• **CVE-2010-3679 MySQL CVSS 2.0 Score = 4.0**

MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via certain arguments to the BINLOG command, which triggers an access of uninitialized memory, as demonstrated by valgrind.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=628062](https://bugzilla.redhat.com/show_bug.cgi?id=628062)

MLIST: <http://www.openwall.com/lists/oss-security/2010/09/28/10>

CONFIRM: <http://bugs.mysql.com/bug.php?id=54393>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html>

**CVE Reference:** [CVE-2010-3679](#)

• **CVE-2010-3680 MySQL CVSS 2.0 Score = 4.0**

MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by creating temporary tables while using InnoDB, which triggers an assertion failure.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=628192](https://bugzilla.redhat.com/show_bug.cgi?id=628192)

MLIST: <http://www.openwall.com/lists/oss-security/2010/09/28/10>

CONFIRM: <http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html>

CONFIRM: <http://bugs.mysql.com/bug.php?id=54044>

**CVE Reference:** [CVE-2010-3680](#)

• **CVE-2011-0314 IBM CVSS 2.0 Score = 6.5**

Heap-based buffer overflow in IBM WebSphere MQ 6.0 before 6.0.2.11 and 7.0 before 7.0.1.5 allows remote authenticated users to execute arbitrary code or cause a denial of service (queue manager crash) by inserting an invalid message into the queue.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/64550>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1Iz81294>

**CVE Reference:** [CVE-2011-0314](#)

## **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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)