

## 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

HP vulnerability will not set your printer on fire. Duqu good at hiding. Java exploit impacting firms. Sharing of cyberthreat information bill receives both praise and criticism.

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

### • HP says security flaw is real, but flames are unlikely

Hewlett-Packard has shot down claims that a vulnerability in some of its printers could be used to set the devices on fire.

Researchers at Columbia University in New York this week said they discovered a flaw in HP LaserJet printers that could allow attackers to steal sensitive documents, gain control of corporate networks, or even set the affected devices on fire.

These exploits could be accomplished because some HP LaserJet printers do not validate the origin of remote firmware updates before applying them, Salvatore Stolfo, a professor of computer science at Columbia who directed the research, told SCMagazineUS.com on Tuesday. That means anyone can reprogram the devices with malicious firmware. SC Magazine

Full Story :

[http://www.scmagazineus.com/hp-says-security-flaw-is-real-but-flames-are-unlikely/article/217911/?utm\\_source=feed](http://www.scmagazineus.com/hp-says-security-flaw-is-real-but-flames-are-unlikely/article/217911/?utm_source=feed)

### • Duqu perpetrators wipe command servers of evidence

The identity of those behind Duqu, the so-called "son of Stuxnet," is still a mystery and the perpetrators have taken pains to keep it that way. On Oct 20, just two days after security firm Symantec first released details about Duqu, the coders behind the information-stealing trojan, which researchers believe shares much of its code with the notorious Stuxnet worm, scrubbed all the files from their command-and-control (C&C) servers in an effort to conceal their identity, according to researchers at anti-virus firm Kaspersky Lab. The C&C servers, used as far back as 2009, were located in India, Vietnam, Germany, the U.K, the Netherlands, Belgium and South Korea, among other countries.

Roel Schouwenberg, senior researcher at Kaspersky Lab, told SCMagazineUS.com in an email Thursday that the attackers' efforts to keep their identity under wraps have undoubtedly made it more difficult for those investigating the threat. SC Magazine

Full Story :

[http://www.scmagazineus.com/duqu-perpetrators-wipe-command-servers-of-evidence/article/217950/?utm\\_source=f](http://www.scmagazineus.com/duqu-perpetrators-wipe-command-servers-of-evidence/article/217950/?utm_source=f)

### • New Java exploit one of many impacting firms

A new exploit for a recently fixed vulnerability in Java has been added to the Metasploit penetration testing framework, according to vulnerability management firm Rapid7, which owns the open-source Metasploit Project.

The exploit takes advantage of a flaw in the Java Runtime Environment (JRE) component in Oracle Java SE JDK and JRE 7 and 6 Update 27 and earlier versions, according to a vulnerability summary. Users can unknowingly become infected simply by visiting a malicious website.

"It's essentially zero-knowledge from the user's perspective," Jonathan Cran, director of quality assurance for the Metasploit Project, told SCMagazineUS.com on Thursday. "It runs on their computer without them even realizing it." SC Magazine

Full Story :

[http://www.scmagazineus.com/new-java-exploit-one-of-many-impacting-firms/article/217974/?utm\\_source=feedburner](http://www.scmagazineus.com/new-java-exploit-one-of-many-impacting-firms/article/217974/?utm_source=feedburner)

### • Bill to foster threat data sharing draws mixed reactions

A bill introduced in the House Intelligence Committee on Wednesday to promote the sharing of cyberthreat information between the public and private sectors has garnered both praise and criticism.

The Cyber Intelligence Sharing and Protection Act of 2011, introduced by the committee's Chairman Mike Rogers, R-Mich., and C.A. "Dutch" Ruppertsberger, D-Md., would give the federal government authority to share classified cyberthreat information with members of the private sector in an effort to help businesses better protect their networks. The legislation would allow enterprises to share threat details with the government anonymously on a voluntarily basis.

"Economic predators, including nation-states, are blatantly stealing business secrets and innovation from private companies," Rogers said in a news release. "This cybersecurity bill goes a long way in helping American businesses better protect their networks and their intellectual property." SC Magazine

Full Story :

[http://www.scmagazineus.com/bill-to-foster-threat-data-sharing-draws-mixed-reactions/article/217979/?utm\\_source=f](http://www.scmagazineus.com/bill-to-foster-threat-data-sharing-draws-mixed-reactions/article/217979/?utm_source=f)

## New Vulnerabilities Tested in SecureScout

### • 19656 Microsoft Windows Untrusted search path vulnerability in Windows Mail and Windows Meeting Space

Untrusted search path vulnerability in Windows Mail and Windows Meeting Space in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .eml or .wcinvt file, aka "Windows Mail Insecure Library Loading Vulnerability."

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

#### References:

\* MS: MS11-085

<http://technet.microsoft.com/security/bulletin/MS11-085>

\* URL: CVE-2011-2016.html

<http://leic.lumension.com/vulnerabilities/2011/CVE-2011-2016.html>

\* URL: detail.php?alert=CVE-2011-2016

<http://www.security-database.com/detail.php?alert=CVE-2011-2016>

**CVE Reference:**

CVE-2011-2016 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19658 Adobe Flash Player arbitrary code via unspecified vectors(CVE-2011-2445)**

Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows and Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-28.html>
- \* BID: 50625  
<http://www.securityfocus.com/bid/50625>
- \* SECUNIA: 2011-2445  
[http://secunia.com/advisories/cve\\_reference/CVE-2011-2445/](http://secunia.com/advisories/cve_reference/CVE-2011-2445/)

**CVE Reference:**

CVE-2011-2445 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19659 Adobe Flash Player arbitrary code via unspecified vectors(CVE-2011-2450)**

Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows and Linux allows attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-28.html>
- \* BID: 50619  
<http://www.securityfocus.com/bid/50619>
- \* SECUNIA: 2011-2450  
[http://secunia.com/advisories/cve\\_reference/CVE-2011-2450/](http://secunia.com/advisories/cve_reference/CVE-2011-2450/)

**CVE Reference:**

CVE-2011-2450 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19660 Adobe Flash Player arbitrary code via unspecified vectors(CVE-2011-2451)**

Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows and Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-28.html>
- \* SECUNIA: 2011-2451  
[http://secunia.com/advisories/cve\\_reference/CVE-2011-2451/](http://secunia.com/advisories/cve_reference/CVE-2011-2451/)
- \* BID: 50623  
<http://www.securityfocus.com/bid/50623>

**CVE Reference:**

CVE-2011-2451 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19661 Adobe Flash Player arbitrary code via unspecified vectors(CVE-2011-2452)**

Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-28.html>
- \* BID: 50622  
<http://www.securityfocus.com/bid/50622>

\* SECUNIA: 2011-2452

[http://secunia.com/advisories/cve\\_reference/CVE-2011-2452/](http://secunia.com/advisories/cve_reference/CVE-2011-2452/)

#### CVE Reference:

CVE-2011-2452 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19662 Adobe Flash Player arbitrary code via unspecified vectors(CVE-2011-2453)

Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-28.html>

\* BID: 50618

<http://www.securityfocus.com/bid/50618>

\* SECUNIA: 2011-2453

[http://secunia.com/advisories/cve\\_reference/CVE-2011-2453/](http://secunia.com/advisories/cve_reference/CVE-2011-2453/)

#### CVE Reference:

CVE-2011-2453 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19663 Adobe Flash Player arbitrary code via unspecified vectors(CVE-2011-2454)

Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

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

#### References:

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-28.html>

\* SECUNIA: 2011-2454

[http://secunia.com/advisories/cve\\_reference/CVE-2011-2454/](http://secunia.com/advisories/cve_reference/CVE-2011-2454/)

\* BID: 50626

<http://www.securityfocus.com/bid/50626>

#### CVE Reference:

CVE-2011-2454 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19664 Apple iTunes execute arbitrary code via a Trojan horse update

iTunes periodically checks for software updates using an HTTP request to Apple.

This request may cause iTunes to indicate that an update is available.

If Apple Software Update for Windows is not installed, clicking the Download iTunes button may open the URL from the HTTP response in the user's default browser.

This issue has been mitigated by using a secured connection when checking for available updates.

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

#### References:

\* FULLDISC: 20080728 Tool release: [evilgrade] - Using DNS cache poisoning to exploit poor update implementations

<http://archives.neohapsis.com/archives/bugtraq/2008-07/0250.html>

\* CONFIRM:

<http://support.apple.com/kb/HT5030>

\* APPLE: APPLE-SA-2011-11-14-1

<http://lists.apple.com/archives/Security-announce/2011/Nov/msg00003.html>

---

Original Advisory:

<http://docs.info.apple.com/article.html?artnum=301596>

Product:

<http://www.apple.com/itunes/>

Other references:

<http://secunia.com/advisories/15310/>

**CVE Reference:**

CVE-2008-3434 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19665 Google Picasa Untrusted search path vulnerability via a Trojan horse**

Google Picasa could allow a remote attacker to execute arbitrary code on the system. The application does not directly specify the fully qualified path to a dynamic-linked library when running on Microsoft Windows. By persuading a victim to open a specially-crafted file from a WebDAV or SMB share using a vulnerable application, a remote attacker could exploit this vulnerability via a specially-crafted library to execute arbitrary code on the system.

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

**References:**

- \* JVN: JVN#99977321  
<http://jvn.jp/en/jp/JVN99977321/index.html>
  - \* JVNDB: JVNDB-2011-000022  
<http://jvndb.jvn.jp/jvndb/JVNDB-2011-000022>
  - \* BID: 47031  
<http://www.securityfocus.com/bid/47031>
  - \* OSVDB: 71281  
<http://osvdb.org/71281>
  - \* SECUNIA: 43853  
<http://secunia.com/advisories/43853>
  - \* VUPEN: ADV-2011-0766  
<http://www.vupen.com/english/advisories/2011/0766>
  - \* XF: google-picasa-dll-code-execution(66295)  
<http://xforce.iss.net/xforce/xfdb/66295>
  - \* JVN: JVNDB-2011-000022.html  
<http://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-000022.html>
- 

Original Advisory:  
<http://docs.info.apple.com/article.html?artnum=301596>

Product:  
<http://www.apple.com/itunes/>

Other references:  
<http://secunia.com/advisories/15310/>

**CVE Reference:**

CVE-2011-0458 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19666 Adobe Flash Player arbitrary code via unspecified vectors(CVE-2011-2455)**

Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb11-28.html>
- \* SECUNIA: CVE-2011-2455  
[http://secunia.com/advisories/cve\\_reference/CVE-2011-2455/](http://secunia.com/advisories/cve_reference/CVE-2011-2455/)
- \* BID: 50627  
<http://www.securityfocus.com/bid/50627>

**CVE Reference:**

CVE-2011-2455 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

- **CVE-2011-4317** Apache CVSS 2.0 Score = 4.3

The mod\_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

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

**References:**

MISC: <https://community.qualys.com/blogs/securitylabs/2011/11/23/apache-reverse-proxy-bypass-issue>

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=756483](https://bugzilla.redhat.com/show_bug.cgi?id=756483)

CONFIRM: <http://thread.gmane.org/gmane.comp.apache.devel/46440>

**CVE Reference:** [CVE-2011-4317](#)

• **CVE-2011-3639 Apache CVSS 2.0 Score = 4.3**

The mod\_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

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

**References:**

CONFIRM: [https://bugzilla.redhat.com/show\\_bug.cgi?id=752080](https://bugzilla.redhat.com/show_bug.cgi?id=752080)

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1188745>

**CVE Reference:** [CVE-2011-3639](#)

• **CVE-2011-4161 HP CVSS 2.0 Score = 10.0**

The default configuration of the HP CM8060 Color MFP with Edgeline; Color LaserJet 3xxx, 4xxx, 5550, 9500, CMxxxx, CPxxxx, and Enterprise CPxxxx; Digital Sender 9200c and 9250c; LaserJet 4xxx, 5200, 90xx, Mxxxx, and Pxxxx; and LaserJet Enterprise 500 color M551, 600, M4555 MFP, and P3015 enables the Remote Firmware Update (RFU) setting, which allows remote attackers to execute arbitrary code by using a session on TCP port 9100 to upload a crafted firmware update.

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

**References:**

MLIST: <https://lists.immunityinc.com/pipermail/dailydave/2011-November/000378.html>

MISC:

<http://redtape.msnbc.msn.com/news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack>

MISC: <http://isc.sans.org/diary/Hacking+HP+Printers+for+Fun+and+Profit/12112>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03102449>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03102449>

**CVE Reference:** [CVE-2011-4161](#)

• **CVE-2011-4668 IBM CVSS 2.0 Score = 7.5**

IBM Tivoli Netcool/Reporter 2.2 before 2.2.0.8 allows remote attackers to execute arbitrary code via vectors related to an unspecified CGI program used with the Apache HTTP Server.

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

**References:**

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1IZ94277>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg24031456>

**CVE Reference:** [CVE-2011-4668](#)

• **CVE-2011-1372 IBM CVSS 2.0 Score = 6.8**

The Web User Interface on the IBM TS3100 and TS3200 tape libraries with firmware before A.60 allows remote attackers to bypass authentication and obtain administrative access via unspecified vectors.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/71026>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=ssg1S1003938>

**CVE Reference:** [CVE-2011-1372](#)

• **CVE-2011-4566 PHP CVSS 2.0 Score = 6.4**

Integer overflow in the exif\_process\_IFD\_TAG function in exif.c in the exif extension in PHP 5.4.0beta2 on 32-bit platforms allows remote attackers to read the contents of arbitrary memory locations or cause a denial of service via a crafted offset\_val value in an EXIF header in a JPEG file, a different vulnerability than CVE-2011-0708.

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

**References:**

CONFIRM: <https://bugs.php.net/bug.php?id=60150>

**CVE Reference:** [CVE-2011-4566](#)

• **CVE-2011-4191 Novell CVSS 2.0 Score = 7.5**

Stack-based buffer overflow in the xdrDecodeString function in XNFS.NLM in Novell NetWare 6.5 SP8 allows remote attackers to execute arbitrary code or cause a denial of service (abend or NFS outage) via long packets.

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

**References:**

CONFIRM: [https://bugzilla.novell.com/show\\_bug.cgi?id=702491](https://bugzilla.novell.com/show_bug.cgi?id=702491)

CONFIRM: [https://bugzilla.novell.com/show\\_bug.cgi?id=671020](https://bugzilla.novell.com/show_bug.cgi?id=671020)

CONFIRM: <http://download.novell.com/Download?buildid=Cfw1tDezgbw~>

**CVE Reference:** [CVE-2011-4191](#)

• **CVE-2011-3173 Novell CVSS 2.0 Score = 7.5**

Stack-based buffer overflow in the GetDriverSettings function in nipplib.dll in the iPrint client in Novell Open Enterprise Server 2 (aka OES2) SP3 allows remote attackers to execute arbitrary code via a long (1) hostname or (2) port field.

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

**References:**

CONFIRM: [https://bugzilla.novell.com/show\\_bug.cgi?id=707730](https://bugzilla.novell.com/show_bug.cgi?id=707730)

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-309/>

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7009676>

CONFIRM: [http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme\\_5117031.html](http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5117031.html)

CONFIRM: [http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme\\_5117030.html](http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5117030.html)

**CVE Reference:** [CVE-2011-3173](#)

**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)