

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

[Mydoom Worm Scanner](#) - The S4 MyDoom 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 the MyDoom email virus or its variants.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=mydoomwormscanner>

This Week in Review

PCI council working on reducing fraud. Digital health and security. Most flaws in web applications. 2nd generation log management.

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

• Visa pilots new payment card security initiatives

March 19, 2009 (Computerworld) Acknowledging the need for controls that go beyond those offered by the Payment Card Industry (PCI) Data Security Standard, a senior Visa Inc. executive today described two new initiatives to reduce payment card fraud being tested by the company.

Another initiative, being piloted by retailer OfficeMax Inc., involves the use of a challenge-response technique at the point of sale. The project is aimed at testing the efficacy of asking consumers to respond to specific questions such as their ZIP code, the last four digits of their phone numbers, or the first three digits of their area codes, as part of the transaction approval process.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130087&source=rss_topic1

• Digital healthcare brings opportunities, risks

March 18, 2009 (Network World) Healthcare in the United States is going digital, which brings both tremendous opportunities and security risks. Digital healthcare brings the promise of increased quality of care, reduced errors and reduced cost and overhead in the provision of care. Yet the United States lags other countries in the use of technology in healthcare records. Fewer than 10% of hospitals and 16% of doctors use electronic health records. This is about to change.

All of this points to an explosion of technology in healthcare and more specifically in the digitization of medical records. With increased digitization, new privacy regulations and more integration between different provider systems bring new risks and an increased burden of regulatory compliance. For security professionals in healthcare this all represents both a tremendous opportunity for skills and career development and a whole load of new responsibilities and work.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9129914&source=rss> topic1

• Web apps account for 80 percent of internet vulnerabilities

Vulnerabilities in web applications made up 80 percent of all web-related flaws in the second half of 2008 and rose in prevalence by about eight percent from the first half of the year, according to a report released Tuesday by Cenizic.

The report was based on the published vulnerability disclosures for various commercial off-the-shelf and open-source software. The web application vulnerabilities, for example, were in Adobe, SAP, Microsoft, Mozilla, Sun, Apache, and Oracle products.

Not securing your web applications is like locking all the doors to your house and leaving the key under a see-through mat, Mandeep Khara, chief marketing officer at Cenizic, which specializes in web application security, told SCMagazineUS.com.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Web-apps-account-for-80-percent-of-internet-vulnerabilities/article/129027/>

• The convergence of SIEM and log management

March 19, 2009 (Network World) Though Security Information and Event Management and log management tools have been complementary for years, the technologies are expected to merge. Here's a look at what you can expect in second-generation log management and SIEM solutions.

The first-generation SIEM technology was designed to reduce this signal-to-noise ratio and help surface the most critical external threats. Using rule-based correlation, SIEM helped IT detect real attacks by focusing on a subset of firewall and IDS/IPS events that were in violation of policy. Traditionally, SIEM solutions have been expensive and time-intensive to maintain and tweak, but they solve the big headache of sorting through excessive false alerts and effectively protect companies from external threats.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130086&source=rss> topic1

New Vulnerabilities Tested in SecureScout

• 18301 Mozilla Firefox - spoof URLs and conduct phishing attacks (Remote File Checking)

Mozilla contributor Masahiro Yamada reported that certain invisible control characters were being decoded when displayed in the location bar, resulting in fewer visible characters than were present in the actual location. An attacker could use this vulnerability to spoof the location bar and display a misleading URL for their malicious web page.

The issue has been fixed in Firefox 3.0.7.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-11.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=452979

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECTRAK: 1021799

<http://securitytracker.com/alerts/2009/Mar/1021799.html>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

* XF: mozilla-invisible-url-spoofing(49087)

<http://xforce.iss.net/xforce/xfdb/49087>

CVE Reference:

CVE-2009-0777 (cve.mitre.org, nvd.nist.gov)

• 18302 Mozilla Firefox - steal arbitrary XML data from another domain (Remote File Checking)

Mozilla security researcher Georgi Guninski reported that a website could use nsIRDFService and a cross-domain redirect to steal arbitrary XML data from another domain, a violation of the same-origin policy. This vulnerability could be used by a malicious website to steal private data from users authenticated to the redirected website.

The issue has been fixed in Firefox 3.0.7.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-09.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=414540

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0776 (cve.mitre.org, nvd.nist.gov)

• 18303 Mozilla Thunderbird - steal arbitrary XML data from another domain (Remote File Checking)

Mozilla security researcher Georgi Guninski reported that a website could use nsIRDFService and a cross-domain redirect to steal arbitrary XML data from another domain, a violation of the same-origin policy. This vulnerability could be used by a malicious website to steal private data from users authenticated to the redirected website.

The issue has been fixed in Thunderbird 2.0.0.21

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-09.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=414540

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0776 (cve.mitre.org, nvd.nist.gov)

• 18304 Mozilla Thunderbird - improper memory management of a set of cloned XUL DOM elements (Remote File Checking)

An anonymous researcher, via TippingPoint's Zero Day Initiative program, reported a vulnerability in Mozilla's garbage collection process. The vulnerability was caused by improper memory management of a set of cloned XUL DOM elements which were linked as a parent and child. After reloading the browser on a page with such linked elements,

the browser would crash when attempting to access an object which was already destroyed. An attacker could use this crash to run arbitrary code on the victim's computer.

The issue has been fixed in Thunderbird 2.0.0.21

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-08.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=474456

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0775 (cve.mitre.org, nvd.nist.gov)

• 18305 Mozilla Firefox - improper memory management of a set of cloned XUL DOM elements (Remote File Checking)

An anonymous researcher, via TippingPoint's Zero Day Initiative program, reported a vulnerability in Mozilla's garbage collection process. The vulnerability was caused by improper memory management of a set of cloned XUL DOM elements which were linked as a parent and child. After reloading the browser on a page with such linked elements, the browser would crash when attempting to access an object which was already destroyed. An attacker could use this crash to run arbitrary code on the victim's computer.

The issue has been fixed in Firefox 3.0.7

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-08.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=474456

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0775 (cve.mitre.org, nvd.nist.gov)

• 18306 Mozilla Firefox - memory corruption (gczeal) (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue affects both Firefox 2.x and 3.x branches.

The issue has been fixed in Firefox 3.0.7

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=473709

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990
<http://www.securityfocus.com/bid/33990>
* SECUNIA: 34145
<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0774 (cve.mitre.org, nvd.nist.gov)

• **18307 Mozilla Thunderbird - memory corruption (gczeal) (Remote File Checking)**

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 2.0.0.21.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=473709
* CONFIRM:
<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>
* BID: 33990
<http://www.securityfocus.com/bid/33990>
* SECUNIA: 34145
<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0774 (cve.mitre.org, nvd.nist.gov)

• **18308 Mozilla Thunderbird - JavaScript engine Denial of Service and Arbitrary Code execution (Remote File Checking)**

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Thunderbird 2.0.0.21.

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

References:

* CONFIRM:
<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=457521
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=467499
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=472787
* CONFIRM:
<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>
* BID: 33990
<http://www.securityfocus.com/bid/33990>
* SECUNIA: 34145
<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0773 (cve.mitre.org, nvd.nist.gov)

• **18309 Mozilla Firefox - JavaScript engine Denial of Service and Arbitrary Code execution (Remote File Checking)**

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue has been fixed in Firefox 3.0.7.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=457521

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=467499

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=472787

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0773 (cve.mitre.org, nvd.nist.gov)

• 18310 Mozilla Firefox - layout engine Denial of Service and Arbitrary Code execution (Remote File Checking)

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

The issue affects Firefox 2.x and 3.x branches.

The issue has been fixed in Firefox 3.0.7.

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

References:

* CONFIRM:

<http://www.mozilla.org/security/announce/2009/mfsa2009-07.html>

* CONFIRM:

https://bugzilla.mozilla.org/show_bug.cgi?id=475136

* CONFIRM:

<http://support.avaya.com/japple/css/japple?temp.documentID=366362&temp.productID=154235&temp.releaseID=361845>

* BID: 33990

<http://www.securityfocus.com/bid/33990>

* SECUNIA: 34145

<http://secunia.com/advisories/34145>

CVE Reference:

CVE-2009-0772 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-0941 HP CVSS 2.0 Score = 7.6

The HP Embedded Web Server (EWS) on HP LaserJet Printers, Edgeline Printers, and Digital Senders has no management password by default, which makes it easier for remote attackers to obtain access.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/501884/100/0/threaded>

MISC: http://www.louhinetworks.fi/advisory/HP_20090317.txt

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01684566>

CVE Reference: [CVE-2009-0941](#)

• **CVE-2009-0940 HP CVSS 2.0 Score = 5.1**

Multiple cross-site request forgery (CSRF) vulnerabilities in the HP Embedded Web Server (EWS) on HP LaserJet Printers, Edgeline Printers, and Digital Senders allow remote attackers to (1) print documents via unknown vectors, (2) modify the network configuration via a NetIPChange request to hp/device/config_result_YesNo.html/config, or (3) change the password via the Password and ConfirmPassword parameters to hp/device/set_config_password.html/config.

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

References:

BID: <http://www.securityfocus.com/bid/34143>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/501884/100/0/threaded>

MISC: http://www.louhinetworks.fi/advisory/HP_20090317.txt

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01684566>

CVE Reference: [CVE-2009-0940](#)

• **CVE-2008-4564 Symantec CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in wp6sr.dll in the Autonomy KeyView SDK 10.4 and earlier, as used in IBM Lotus Notes, Symantec Mail Security (SMS) products, Symantec BrightMail Appliance products, and Symantec Data Loss Prevention (DLP) products, allows remote attackers to execute arbitrary code via a crafted Word Perfect Document (WPD) file.

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

References:

CONFIRM:

https://customers.autonomy.com/support/secure/docs/Updates/Keyview/Filter%20SDK/10.4/kv_update_nti40_10.4.zip.readme

XF: <http://xforce.iss.net/xforce/xfdb/49284>

VUPEN: <http://www.vupen.com/english/advisories/2009/0744>

CONFIRM: <http://www.symantec.com/avcenter/security/Content/2009.03.17a.html>

BID: <http://www.securityfocus.com/bid/34086>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?rs=463&uid=swg21377573>

SECTRAK: <http://securitytracker.com/id?1021857>

SECTRAK: <http://securitytracker.com/id?1021856>

SECUNIA: <http://secunia.com/advisories/34307>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=774>

CVE Reference: [CVE-2008-4564](#)

• **CVE-2009-0538 Symantec CVSS 2.0 Score = 4.6**

Format string vulnerability in Symantec pcAnywhere before 12.5 SP1 allows local users to read and modify arbitrary memory locations, and cause a denial of service (application crash) or possibly have unspecified other impact, via format string specifiers in the pathname of a remote control file (aka .CHF file).

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

References:

CONFIRM: <http://securityresponse.symantec.com/avcenter/security/Content/2009.03.17.html>

XF: <http://xforce.iss.net/xforce/xfdb/49291>

BID: <http://www.securityfocus.com/bid/33845>

MISC: <http://www.layereddefense.com/pcanywhere17mar.html>

SECTRAK: <http://securitytracker.com/id?1021855>

CVE Reference: [CVE-2009-0538](#)

• **CVE-2008-4564 IBM CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in wp6sr.dll in the Autonomy KeyView SDK 10.4 and earlier, as used in IBM Lotus Notes, Symantec Mail Security (SMS) products, Symantec BrightMail Appliance products, and Symantec Data Loss Prevention (DLP) products, allows remote attackers to execute arbitrary code via a crafted Word Perfect Document (WPD) file.

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

References:

CONFIRM:

https://customers.autonomy.com/support/secure/docs/Updates/Keyview/Filter%20SDK/10.4/kv_update_nti40_10.4.zip.rea

XF: <http://xforce.iss.net/xforce/xfdb/49284>

VUPEN: <http://www.vupen.com/english/advisories/2009/0744>

CONFIRM: <http://www.symantec.com/avcenter/security/Content/2009.03.17a.html>

BID: <http://www.securityfocus.com/bid/34086>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?rs=463&uid=swg21377573>

SECTRAK: <http://securitytracker.com/id?1021857>

SECTRAK: <http://securitytracker.com/id?1021856>

SECUNIA: <http://secunia.com/advisories/34307>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=774>

CVE Reference: [CVE-2008-4564](#)

• **CVE-2009-0508 IBM CVSS 2.0 Score = 5.0**

The Servlet Engine/Web Container component in IBM WebSphere Application Server (WAS) 5.1.0, 5.1.1.19, 6.0.2 before 6.0.2.35, 6.1 before 6.1.0.23, and 7.0 before 7.0.0.3 allows remote attackers to read arbitrary files contained in war files in (1) web-inf, (2) meta-inf, and unspecified other directories via unknown vectors, related to (a) web-based applications and (b) the administrative console.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24022456>

XF: <http://xforce.iss.net/xforce/xfdb/49085>

BID: <http://www.securityfocus.com/bid/34104>

CVE Reference: [CVE-2009-0508](#)

• **CVE-2009-0927 Adobe CVSS 2.0 Score = 10.0**

Unspecified vulnerability in Adobe Reader and Adobe Acrobat 9.1 and 7.1.1 allows remote attackers to execute arbitrary code via unknown vectors related to a JavaScript method and input validation, a different vulnerability than CVE-2009-0658.

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

References:

BID: <http://www.securityfocus.com/bid/34169>

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb09-04.html>

CVE Reference: [CVE-2009-0927](#)

- **CVE-2009-0923 Sun CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Kerberos Incremental Propagation in Solaris 10 and OpenSolaris snv_01 through snv_110 allows remote attackers to cause a denial of service (loss of incremental propagation requests to slave KDC servers) via unknown vectors related to the master Key Distribution Center (KDC) server.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/0741>

BID: <http://www.securityfocus.com/bid/34139>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-249926-1>

SECUNIA: <http://secunia.com/advisories/34298>

CVE Reference: [CVE-2009-0923](#)

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