

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

This week, the team behind the SC Magazine Best Buy vulnerability scanner - yours truly, implemented a series of enhancements to the framework used by the Authenticated Scan Remote File Check test method. The enhancements resulted in (1) a lighter memory footprint, (2) better test accuracy by checking more default locations, (3) faster execution by using a more robust caching methodology, (4) faster execution by eventually skipping tests of some default locations if possible.

Fraudulent ssl certificates. US alerts about vulnerabilities in industry used control software. Fraudulent ssl certificates used inherent internet design chink. European Commission under cyber attack..

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

• Experts weigh in on Comodo SSL certificate fraud

Reactions are running rampant after security firm Comodo revealed it was tricked into issuing rogue digital certificates, with some speculating that Iranian hackers launched the attack to facilitate government monitoring of citizens and others using the incident to highlight what they call inherent flaws in the SSL certificate ecosystem.

Comodo, a Jersey City, N.J.-based company that issues digital SSL certificates used by websites to validate their identity to visitors, disclosed Wednesday that it had mistakenly issued nine fraudulent certificates for big name sites like Google, Yahoo, Skype and Microsoft's Hotmail. The certificates could have allowed attackers to set up fake versions of the sites and collect usernames and passwords, or read users' email messages, researchers have warned.

Evidence indicates that the attack was state sponsored, according to Comodo. SC Magazine

Full Story :

http://www.scmagazineus.com/experts-weigh-in-on-comodo-ssl-certificate-fraud/article/199109/?utm_source=feedbu

• U.S. government warns of SCADA flaws

Following disclosures earlier this week about vulnerabilities in supervisory control and data acquisition software (SCADA) systems, US-CERT issued alerts for four different software products used to control hardware appliances at such industrial facilities as nuclear plants and gas refineries. On Monday, Luigi Auriemma, a 30-year-old Italian independent researcher, posted the advisories and proof-of-concepts to the Bugtraq email mailing list.

Auriemma explained that at least 34 vulnerabilities - found in programs sold by Siemens, Iconics, 7-Technologies, Datac and Control Microsystems - allow people to monitor and control the various hardware sensors and mechanisms located in industrial environments and could enable attackers to remotely execute code and targeted attacks via buffer and heap overflows. SC Magazine

Full Story :

http://www.scmagazineus.com/us-government-warns-of-scada-flaws/article/198974/?utm_source=feedburner&utm_r

• Hackers exploit chink in Web's armor

A long-known but little-discussed vulnerability in the modern Internet's design was highlighted yesterday by a report that hackers traced to Iran spoofed the encryption procedures used to secure connections to Google, Yahoo, Microsoft, and other major Web sites.

This design, pioneered by Netscape in the early and mid-1990s, allows the creation of encrypted channels to Web sites, an important security feature typically identified by a closed lock icon in a browser. The system relies on third parties to issue so-called certificates that prove that a Web site is legitimate when making an "https://" connection.

The problem, however, is that the list of certificate issuers has ballooned over the years to approximately 650 organizations, which may not always follow the strictest security procedures. And each one has a copy of the Web's master keys. Cnet Security

Full Story :

http://news.cnet.com/8301-31921_3-20046588-281.html?part=rss&subj=news&tag=2547-1_3-0-20

• European Commission hit by cyberattack

IDG News Service - The European Commission, including the body's diplomatic arm, has been hit by what officials said Thursday was a serious cyberattack.

The attack was first detected on Tuesday and commission sources have said that it was sustained and targeted.

External access to the commission's e-mail and intranet has been suspended and staff have been told to change their passwords in order to prevent the "disclosure of unauthorized information," according to an internal memo to staff. Staff at the commission, the European Union's executive and regulatory body, have also been told to send sensitive information via secure e-mail. Computerworld

Full Story :

http://www.computerworld.com/s/article/9215041/European_Commission_hit_by_cyberattack?source=rss_security&

New Vulnerabilities Tested in SecureScout

• 19224 Adobe Flash Player library-loading vulnerability (CVE-2011-0575) (Remote File Checking)

Untrusted search path vulnerability in Adobe Flash Player before 10.2.152.26 allows local users to gain privileges via a Trojan horse DLL in the current working directory.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

- * BUGTRAQ: 20110211 ASPR #2011-02-11-2: Remote Binary Planting in Adobe Flash Player
<http://www.securityfocus.com/archive/1/archive/1/516398/100/0/threaded>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
- * REDHAT: RHSA-2011:0206

<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
* REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
* SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
* BID: 46197
<http://www.securityfocus.com/bid/46197>
* OSVDB: 70919
<http://osvdb.org/70919>
* SECTRACK: 1025055
<http://www.securitytracker.com/id?1025055>
* SECUNIA: 43267
<http://secunia.com/advisories/43267>
* SECUNIA: 43292
<http://secunia.com/advisories/43292>
* SECUNIA: 43340
<http://secunia.com/advisories/43340>
* SECUNIA: 43351
<http://secunia.com/advisories/43351>
* VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
* VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
* VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>
* XF: adobe-flash-dll-code-exec(65238)
<http://xforce.iss.net/xforce/xfdb/65238>

CVE Reference:

CVE-2011-0575 (cve.mitre.org, nvd.nist.gov)

● 19225 Adobe Flash Player font-parsing vulnerability (CVE-2011-0577) (Remote File Checking)

Unspecified vulnerability in Adobe Flash Player before 10.2.152.26 allows remote attackers to execute arbitrary code via a crafted font.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
* REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
* REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
* SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
* BID: 46196
<http://www.securityfocus.com/bid/46196>
* OSVDB: 70920
<http://osvdb.org/70920>
* SECTRACK: 1025055
<http://www.securitytracker.com/id?1025055>
* SECUNIA: 43267
<http://secunia.com/advisories/43267>
* SECUNIA: 43292
<http://secunia.com/advisories/43292>
* SECUNIA: 43340
<http://secunia.com/advisories/43340>
* SECUNIA: 43351
<http://secunia.com/advisories/43351>
* VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
* VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
* VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>

* XF: adobe-fontprasing-code-execution(65239)
<http://xforce.iss.net/xforce/xfdb/65239>

CVE Reference:

CVE-2011-0577 (cve.mitre.org, nvd.nist.gov)

• 19226 Adobe Flash Player memory corruption vulnerability (CVE-2011-0578) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors related to a constructor for an unspecified ActionScript3 object and improper type checking, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0607, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-11-081/>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-02.html>

* REDHAT: RHSA-2011:0206

<http://www.redhat.com/support/errata/RHSA-2011-0206.html>

* REDHAT: RHSA-2011:0259

<http://www.redhat.com/support/errata/RHSA-2011-0259.html>

* SUSE: SUSE-SA:2011:009

<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>

* OSVDB: 70921

<http://osvdb.org/70921>

* SECTRACK: 1025055

<http://www.securitytracker.com/id?1025055>

* SECUNIA: 43267

<http://secunia.com/advisories/43267>

* SECUNIA: 43292

<http://secunia.com/advisories/43292>

* SECUNIA: 43340

<http://secunia.com/advisories/43340>

* SECUNIA: 43351

<http://secunia.com/advisories/43351>

* VUPEN: ADV-2011-0348

<http://www.vupen.com/english/advisories/2011/0348>

* VUPEN: ADV-2011-0383

<http://www.vupen.com/english/advisories/2011/0383>

* VUPEN: ADV-2011-0402

<http://www.vupen.com/english/advisories/2011/0402>

* XF: adobe-flashplayer-unspec-ce(65240)

<http://xforce.iss.net/xforce/xfdb/65240>

CVE Reference:

CVE-2011-0578 (cve.mitre.org, nvd.nist.gov)

• 19227 Adobe Flash Player memory corruption vulnerability (CVE-2011-0607) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, and CVE-2011-0608.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-02.html>

* REDHAT: RHSA-2011:0206

<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
* REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
* SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
* BID: 46282
<http://www.securityfocus.com/bid/46282>
* OSVDB: 70922
<http://osvdb.org/70922>
* SECTRACK: 1025055
<http://www.securitytracker.com/id?1025055>
* SECUNIA: 43267
<http://secunia.com/advisories/43267>
* SECUNIA: 43292
<http://secunia.com/advisories/43292>
* SECUNIA: 43340
<http://secunia.com/advisories/43340>
* SECUNIA: 43351
<http://secunia.com/advisories/43351>
* VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
* VUPEN: ADV-2011-0383
<http://www.vupen.com/english/advisories/2011/0383>
* VUPEN: ADV-2011-0402
<http://www.vupen.com/english/advisories/2011/0402>
* XF: adobe-player-ce(65241)
<http://xforce.iss.net/xforce/xfdb/65241>

CVE Reference:

CVE-2011-0607 (cve.mitre.org, nvd.nist.gov)

● 19228 Adobe Flash Player memory corruption vulnerability (CVE-2011-0608) (Remote File Checking)

Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, and CVE-2011-0607.

Adobe Flash Player version 10.2.152.26 resolves the issue.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-02.html>
* REDHAT: RHSA-2011:0206
<http://www.redhat.com/support/errata/RHSA-2011-0206.html>
* REDHAT: RHSA-2011:0259
<http://www.redhat.com/support/errata/RHSA-2011-0259.html>
* SUSE: SUSE-SA:2011:009
<http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00003.html>
* BID: 46283
<http://www.securityfocus.com/bid/46283>
* OSVDB: 70923
<http://osvdb.org/70923>
* SECTRACK: 1025055
<http://www.securitytracker.com/id?1025055>
* SECUNIA: 43267
<http://secunia.com/advisories/43267>
* SECUNIA: 43292
<http://secunia.com/advisories/43292>
* SECUNIA: 43340
<http://secunia.com/advisories/43340>
* SECUNIA: 43351
<http://secunia.com/advisories/43351>
* VUPEN: ADV-2011-0348
<http://www.vupen.com/english/advisories/2011/0348>
* VUPEN: ADV-2011-0383

<http://www.vupen.com/english/advisories/2011/0383>

* VUPEN: ADV-2011-0402

<http://www.vupen.com/english/advisories/2011/0402>

* XF: adobe-code-exec(65242)

<http://xforce.iss.net/xforce/xfdb/65242>

CVE Reference:

CVE-2011-0608 (cve.mitre.org, nvd.nist.gov)

• 19229 Adobe Acrobat / Reader 'SWF' File Remote Memory Corruption Vulnerability (Remote File Checking)

A critical vulnerability exists in Adobe Flash Player 10.2.152.33 and earlier versions for Windows, Macintosh, Linux and Solaris operating systems (Adobe Flash Player 10.2.154.18 and earlier for Chrome users), Adobe Flash Player 10.1.106.16 and earlier versions for Android, and the authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.1) and earlier 10.x and 9.x versions for Windows and Macintosh operating systems.

This vulnerability (CVE-2011-0609) could cause a crash and potentially allow an attacker to take control of the affected system. There are reports that this vulnerability is being exploited in the wild in targeted attacks via a Flash (.swf) file embedded in a Microsoft Excel (.xls) file delivered as an email attachment. Adobe is not currently aware of attacks targeting Adobe Reader and Acrobat. Adobe Reader X Protected Mode mitigations would prevent an exploit of this kind from executing.

Adobe Reader and Acrobat X versions 9.4.3, and 10.0.2, resolve the issue.

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

References:

* BID: 46860

<http://www.securityfocus.com/bid/46860>

* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa11-01.html>

* CONFIRM:

<http://blogs.adobe.com/asset/2011/03/background-on-apsa11-01-patch-schedule.html>

CVE Reference:

CVE-2011-0609 (cve.mitre.org, nvd.nist.gov)

• 19230 Adobe Flash Player input validation issue vulnerability (Remote File Checking)

Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, does not properly handle unspecified encodings during the parsing of a cross-domain policy file, which allows remote web servers to bypass intended access restrictions via unknown vectors.

Adobe Flash Player versions 9.0.289.0, and 10.1.102.64 resolve the issue.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-26.html>

* CONFIRM:

<http://support.apple.com/kb/HT4435>

* CONFIRM:

http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_adobe_flash1

* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>

* GENTOO: GLSA-201101-09

<http://security.gentoo.org/glsa/glsa-201101-09.xml>

* REDHAT: RHSA-2010:0829

<http://www.redhat.com/support/errata/RHSA-2010-0829.html>

* REDHAT: RHSA-2010:0834

<http://www.redhat.com/support/errata/RHSA-2010-0834.html>

* REDHAT: RHSA-2010:0867

<http://www.redhat.com/support/errata/RHSA-2010-0867.html>

* SUSE: SUSE-SA:2010:055

<http://lists.opensuse.org/opensuse-security-announce/2010-11/msg00002.html>

* JVN: JVN#48425028

<http://jvn.jp/en/jp/JVN48425028/index.html>

* JVNDB: JVNDB-2010-000054
<http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-000054.html>
* BID: 44691
<http://www.securityfocus.com/bid/44691>
* SECUNIA: 42183
<http://secunia.com/advisories/42183>
* SECUNIA: 42926
<http://secunia.com/advisories/42926>
* SECUNIA: 43026
<http://secunia.com/advisories/43026>
* VUPEN: ADV-2010-2903
<http://www.vupen.com/english/advisories/2010/2903>
* VUPEN: ADV-2010-2906
<http://www.vupen.com/english/advisories/2010/2906>
* VUPEN: ADV-2010-2918
<http://www.vupen.com/english/advisories/2010/2918>
* VUPEN: ADV-2011-0173
<http://www.vupen.com/english/advisories/2011/0173>
* VUPEN: ADV-2011-0192
<http://www.vupen.com/english/advisories/2011/0192>

CVE Reference:

CVE-2010-3636 (cve.mitre.org, nvd.nist.gov)

• 19231 Adobe Flash Player memory corruption vulnerability (Remote File Checking)

An unspecified ActiveX control in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 (Flash10h.ocx) on Windows allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FLV video.

Adobe Flash Player versions 9.0.289.0, and 10.1.102.64 resolve the issue.

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

References:

* BUGTRAQ: 20101105 [FG-VD-10-020]Adobe Flash Player Remote Memory corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/514652/100/0/threaded>
* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-26.html>
* CONFIRM:
http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_adobe_flash1
* SUSE: SUSE-SA:2010:055
<http://lists.opensuse.org/opensuse-security-announce/2010-11/msg00002.html>
* BID: 44690
<http://www.securityfocus.com/bid/44690>
* SECUNIA: 42926
<http://secunia.com/advisories/42926>
* VUPEN: ADV-2010-2903
<http://www.vupen.com/english/advisories/2010/2903>
* VUPEN: ADV-2011-0173
<http://www.vupen.com/english/advisories/2011/0173>

CVE Reference:

CVE-2010-3637 (cve.mitre.org, nvd.nist.gov)

• 19233 Adobe Flash Player arbitrary code execution vulnerability (Remote File Checking)

Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.

Adobe Flash Player versions 9.0.289.0, and 10.1.102.64 resolve the issue.

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

References:

* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb10-26.html>
* CONFIRM:

<http://support.apple.com/kb/HT4435>

* CONFIRM:

http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_adobe_flash1

* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>

* GENTOO: GLSA-201101-09

<http://security.gentoo.org/glsa/glsa-201101-09.xml>

* REDHAT: RHSA-2010:0829

<http://www.redhat.com/support/errata/RHSA-2010-0829.html>

* REDHAT: RHSA-2010:0834

<http://www.redhat.com/support/errata/RHSA-2010-0834.html>

* REDHAT: RHSA-2010:0867

<http://www.redhat.com/support/errata/RHSA-2010-0867.html>

* SUSE: SUSE-SA:2010:055

<http://lists.opensuse.org/opensuse-security-announce/2010-11/msg00002.html>

* BID: 44692

<http://www.securityfocus.com/bid/44692>

* SECUNIA: 42183

<http://secunia.com/advisories/42183>

* SECUNIA: 42926

<http://secunia.com/advisories/42926>

* SECUNIA: 43026

<http://secunia.com/advisories/43026>

* VUPEN: ADV-2010-2903

<http://www.vupen.com/english/advisories/2010/2903>

* VUPEN: ADV-2010-2906

<http://www.vupen.com/english/advisories/2010/2906>

* VUPEN: ADV-2010-2918

<http://www.vupen.com/english/advisories/2010/2918>

* VUPEN: ADV-2011-0173

<http://www.vupen.com/english/advisories/2011/0173>

* VUPEN: ADV-2011-0192

<http://www.vupen.com/english/advisories/2011/0192>

CVE Reference:

CVE-2010-3639 (cve.mitre.org, nvd.nist.gov)

• 19234 Adobe Flash Player memory corruption vulnerability (CVE-2010-3640) (Remote File Checking)

Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.

Adobe Flash Player versions 9.0.289.0, and 10.1.102.64 resolve the issue.

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

References:

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb10-26.html>

* CONFIRM:

<http://support.apple.com/kb/HT4435>

* CONFIRM:

http://blogs.sun.com/security/entry/multiple_vulnerabilities_in_adobe_flash1

* APPLE: APPLE-SA-2010-11-10-1

<http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html>

* GENTOO: GLSA-201101-09

<http://security.gentoo.org/glsa/glsa-201101-09.xml>

* REDHAT: RHSA-2010:0829

<http://www.redhat.com/support/errata/RHSA-2010-0829.html>

* REDHAT: RHSA-2010:0834

<http://www.redhat.com/support/errata/RHSA-2010-0834.html>

* REDHAT: RHSA-2010:0867

<http://www.redhat.com/support/errata/RHSA-2010-0867.html>

* SUSE: SUSE-SA:2010:055

<http://lists.opensuse.org/opensuse-security-announce/2010-11/msg00002.html>

* BID: 44675
<http://www.securityfocus.com/bid/44675>
* SECUNIA: 42183
<http://secunia.com/advisories/42183>
* SECUNIA: 42926
<http://secunia.com/advisories/42926>
* SECUNIA: 43026
<http://secunia.com/advisories/43026>
* VUPEN: ADV-2010-2903
<http://www.vupen.com/english/advisories/2010/2903>
* VUPEN: ADV-2010-2906
<http://www.vupen.com/english/advisories/2010/2906>
* VUPEN: ADV-2010-2918
<http://www.vupen.com/english/advisories/2010/2918>
* VUPEN: ADV-2011-0173
<http://www.vupen.com/english/advisories/2011/0173>
* VUPEN: ADV-2011-0192
<http://www.vupen.com/english/advisories/2011/0192>

CVE Reference:

CVE-2010-3640 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1505 IBM CVSS 2.0 Score = 10.0

Unspecified vulnerability in IBM Lotus Quickr 8.1 before 8.1.0.27 services for Lotus Domino has unknown impact and attack vectors, aka SPR ESEO8DQME2.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/66142>
BID: <http://www.securityfocus.com/bid/46903>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1LO58209>
CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27013341>
SECTrack: <http://securitytracker.com/id?1025228>
SECUNIA: <http://secunia.com/advisories/43689>

CVE Reference: [CVE-2011-1505](http://cve.mitre.org/cve/2011/1505)

• CVE-2008-7285 IBM CVSS 2.0 Score = 5.0

Unspecified vulnerability in the docnote string handling implementation in IBM Lotus Quickr 8.1 before 8.1.0.2 services for Lotus Domino allows remote attackers to cause a denial of service (daemon crash) via unknown vectors, aka SPR JFLD7GZT25.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27013341>

CVE Reference: [CVE-2008-7285](http://cve.mitre.org/cve/2008/7285)

• CVE-2009-5059 IBM CVSS 2.0 Score = 4.0

Unspecified vulnerability in IBM Lotus Quickr 8.1 before 8.1.0.10 services for Lotus Domino might allow remote authenticated users to cause a denial of service (daemon crash) by checking out a document that is accessed through a connector, aka SPR MMOI7PSR8J.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27013341>

CVE Reference: [CVE-2009-5059](#)

• **CVE-2008-7286 IBM CVSS 2.0 Score = 4.0**

IBM Lotus Quickr 8.1 before 8.1.0.2 services for Lotus Domino does not properly handle URLs that request images, which allows remote authenticated users to cause a denial of service (daemon crash) via a request to resources.nsf, aka SPR XFXF7JDBCX.

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

References:

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg27013341>

CVE Reference: [CVE-2008-7286](#)

• **CVE-2011-1467 PHP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.

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

References:

CONFIRM: <http://bugs.php.net/bug.php?id=53512>

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

CVE Reference: [CVE-2011-1467](#)

• **CVE-2011-1466 PHP CVSS 2.0 Score = 5.0**

Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

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

References:

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

CONFIRM: <http://bugs.php.net/bug.php?id=53574>

CVE Reference: [CVE-2011-1466](#)

• **CVE-2010-4228 Novell CVSS 2.0 Score = 9.0**

Stack-based buffer overflow in NWFTPD.NLM before 5.10.02 in the FTP server in Novell NetWare allows remote authenticated users to execute arbitrary code or cause a denial of service (abend) via a long DELE command, a different vulnerability than CVE-2010-0625.4.

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

References:

CONFIRM: https://bugzilla.novell.com/show_bug.cgi?id=641249

XF: <http://xforce.iss.net/xforce/xfdb/66170>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-11-106/>

BID: <http://www.securityfocus.com/bid/46922>

MISC: http://www.protekresearchlab.com/index.php?option=com_content&view=article&id=25&Itemid=25

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=3238588>

SECUNIA: <http://secunia.com/advisories/43824>

CVE Reference: [CVE-2010-4228](#)

• **CVE-2011-0173 Apple CVSS 2.0 Score = 7.5**

Multiple format string vulnerabilities in AppleScript in Apple Mac OS X before 10.6.7 allow context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via format string specifiers in a (1) display dialog or (2) display alert command in a dialog in an AppleScript Studio application.

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

References:

CONFIRM: <http://support.apple.com/kb/HT4581>

APPLE: <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>

CVE Reference: [CVE-2011-0173](https://cve.mitre.org/cve/2011/0173)

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