ScoutNews
The weekly Security update from the makers of SecureScout
April 01, 2011

2011 Issue #13

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

Restaurant chain agrees to increase security. 21st century security must engage employees. SSL fraud spreading. Crime focus shifting from individuals to corporate.

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

- **Restaurant chain to pay $110,000 to settle breach claims**

Computerworld - The Briar Group, which operates several restaurants in the Boston area, has agreed to pay $110,000 to settle allegations by the Massachusetts Attorney General's office that it failed to take reasonable steps to protect credit card data belonging to tens of thousands of customers.

Under terms of the settlement, announced Monday, the Briar Group also agreed to implement a strong password management system at each of its restaurants and to comply with the Payment Card Industry Data Security Standard.

The settlement relates to an incident that began in April 2009 when intruders broke into a Briar Group computer and installed malware designed to steal credit and debit card data. According to a lawsuit filed in Suffolk Superior Court by Attorney General Martha Coakley, the malicious software wasn't removed in Dec. 2009. Computerworld

Full Story :
http://www.computerworld.com/s/article/9215299/Restaurant_chain_to_pay_110_000_to_settle_breach_claims?sourc

- **Security in 3D**

CSO - Managing security complexity is the number one obstacle that enterprises face today, according to a recent Check Point and Ponemon Institute survey of over 2,400 IT security professionals. With the prevalence of data loss and the proliferation of Web 2.0 applications, mobile computing and the rise of sophisticated, blended attacks, it is no wonder that businesses--regardless of their size--are struggling to keep up with the evolving threat landscape.

More and more companies are realizing that security must be a more central part of their overall IT infrastructure, to achieve the level of protection that they need in the twenty-first century business environments, companies should consider implementing a blueprint for security that goes beyond technology and can engage employees in the security process, and ultimately, helping organizations align their IT policies with their business needs.

Also read Jennifer Bayuk's How to write an information security policy Computerworld

Full Story :
http://www.computerworld.com/s/article/9215341/Security_in_3D?source=rss_security&utm_source=feedburner&utr

- **Two more Comodo resellers "owned" in SSL hack**

Comodo has confirmed that two additional registration authorities (RAs) affiliated with the company also were compromised in a highly publicized SSL certificate fraud attack disclosed last week.

No additional forged certificates were issued as a result of the latest compromises, according to Comodo. Further, the company has suspended the registration authority privileges of its two latest affected resellers.

Robin Alden, CTO of Comodo, announced the new compromises on a Mozilla web group discussion thread that was created after the initial attack. SC Magazine

Full Story :
http://www.scmagazineus.com/two-more-comodo-resellers-owned-in-ssl-hack/article/199620/?utm_source=feedburn

- **Corporate data is new target of cybercrime**

Cybercriminals have shifted their efforts from targeting individuals' personal information to the intellectual capital of global corporations, according to a report released Monday by McAfee and defense contractor Science Applications International Corp. (SAIC).

The study of more than 1,000 senior IT executives from a wide range of corporations in the United States, U.K., Japan, China, India, Brazil and the Middle East, revealed that intellectual capital often has little to no protection. Moreover, cybercriminals have found that trade secrets, marketing plans and research and development findings is oftentimes worth more money than personal data, such as credit card numbers and bank credentials.

Simon Hunt, vice president and CTO of endpoint security at McAfee, told SCMagazineUS.com that the shift in cybercriminals' focus is a natural evolution. SC Magazine

Full Story :
http://www.scmagazineus.com/corporate-data-is-new-target-of-cybercrime/article/199420/?utm_source=feedburner&

New Vulnerabilities Tested in SecureScout

- **19235 Adobe Flash Player memory corruption vulnerability (CVE-2010-3641) (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-2010-3640, 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: 44677
http://www.securityfocus.com/bid/44677
* 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-2010-3641 (cve.mitre.org, nvd.nist.gov)

• 19236 Adobe Flash Player memory corruption vulnerability (CVE-2010-3642) (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-2010-3640, CVE-2010-3641, 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: 44678
http://www.securityfocus.com/bid/44678

* 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-2010-3642 (cve.mitre.org, nvd.nist.gov)

• 19237 Adobe Flash Player memory corruption vulnerability (CVE-2010-3643) (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-2010-3640, CVE-2010-3641, CVE-2010-3642, 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: 44679
http://www.securityfocus.com/bid/44679
* 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-2010-3643 (cve.mitre.org, nvd.nist.gov)

• 19238 Adobe Flash Player memory corruption vulnerability (CVE-2010-3644) (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-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, 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: 44680
http://www.securityfocus.com/bid/44680
* 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-2010-3644 (cve.mitre.org, nvd.nist.gov)

• 19239 Adobe Flash Player memory corruption vulnerability (CVE-2010-3645) (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-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, 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: 44681
http://www.securityfocus.com/bid/44681
* 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-2010-3645 (cve.mitre.org, nvd.nist.gov)

• 19240 Adobe Flash Player memory corruption vulnerability (CVE-2010-3646) (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-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, 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: 44682
http://www.securityfocus.com/bid/44682
* 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-2010-3646 (cve.mitre.org, nvd.nist.gov)

• 19241 Adobe Flash Player memory corruption vulnerability (CVE-2010-3647) (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-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, 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: 44682
http://www.securityfocus.com/bid/44682
* 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-2010-3647 (cve.mitre.org, nvd.nist.gov)

• 19242 Adobe Flash Player memory corruption vulnerability (CVE-2010-3648) (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-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, 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: 44684
http://www.securityfocus.com/bid/44684
* 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-2010-3648 (cve.mitre.org, nvd.nist.gov)

• 19243 Adobe Flash Player memory corruption vulnerability (CVE-2010-3649) (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-2010-3640, 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-2010-3650, 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: 44685
http://www.securityfocus.com/bid/44685
* 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-2010-3649 (cve.mitre.org, nvd.nist.gov)

• 19244 Adobe Flash Player memory corruption vulnerability (CVE-2010-3650) (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-2010-3640, 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, 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: 44686
http://www.securityfocus.com/bid/44686
* 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-2010-3650 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1420 Oracle CVSS 2.0 Score = 7.2

EMC Data Protection Advisor Collector 5.7 and 5.7.1 on Solaris SPARC platforms uses weak permissions for unspecified files, which allows local users to gain privileges via unknown vectors.

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

References:

BID: http://www.securityfocus.com/bid/47036

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/517179/100/0/threaded

SECTRACK: http://securitytracker.com/id?1025253

CVE Reference: CVE-2011-1420

• CVE-2011-0892 HP CVSS 2.0 Score = 4.3

Cross-site scripting (XSS) vulnerability in HP Diagnostics 7.5x and 8.0x before 8.05.54.225 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.

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

References:

SECTRACK: http://securitytracker.com/id?1025255

SECUNIA: http://secunia.com/advisories/43899

HP: http://marc.info/?l=bugtraq&m=130132024016475&w=2

HP: http://marc.info/?l=bugtraq&m=130132024016475&w=2

CVE Reference: CVE-2011-0892

- **CVE-2011-0545 Symantec CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in adduser.do in Symantec LiveUpdate Administrator (LUA) before 2.3 allows remote attackers to hijack the authentication of administrators for requests that create new administrative accounts, and possibly have unspecified other impact, via the userRole parameter.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/66213

VUPEN: http://www.vupen.com/english/advisories/2011/0727

CONFIRM: http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_adv

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/517109/100/0/threaded

OSVDB: http://www.osvdb.org/71261

EXPLOIT-DB: http://www.exploit-db.com/exploits/17026

MISC: http://sotiriu.de/adv/NSOADV-2011-001.txt

SECTRACK: http://securitytracker.com/id?1025242

SECUNIA: http://secunia.com/advisories/43820

CVE Reference: CVE-2011-0545

- **CVE-2011-1524 Symantec CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in the management login GUI page in Symantec LiveUpdate Administrator (LUA) before 2.3 allows remote attackers to inject arbitrary web script or HTML via the username field, as demonstrated by injecting an IFRAME element into the event log, a different vulnerability than CVE-2011-0545.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/66213

VUPEN: http://www.vupen.com/english/advisories/2011/0727

CONFIRM: http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_adv

BID: http://www.securityfocus.com/bid/46856

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/517109/100/0/threaded

EXPLOIT-DB: http://www.exploit-db.com/exploits/17026

MISC: http://sotiriu.de/adv/NSOADV-2011-001.txt

SECTRACK: http://securitytracker.com/id?1025242

CVE Reference: CVE-2011-1524

- **CVE-2011-1205 IBM CVSS 2.0 Score = 6.9**

Multiple buffer overflows in unspecified COM objects in Rational Common Licensing 7.0 through 7.1.1.4 in IBM Rational ClearCase 7.0.0.4 through 7.1.1.4, ClearQuest 7.0.0.4 through 7.1.1.4, and other products allow local users to gain privileges via a Trojan horse HTML document in the My Computer zone.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/66324

XF: http://xforce.iss.net/xforce/xfdb/66304

CONFIRM: http://www.ibm.com/support/docview.wss?uid=swg21470998

CVE Reference: CVE-2011-1205

- **CVE-2011-0441 PHP CVSS 2.0 Score = 6.3**

The Debian GNU/Linux /etc/cron.d/php5 cron job for PHP 5.3.5 allows local users to delete arbitrary files via a symlink attack on a directory under /var/lib/php5/.

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

References:

CONFIRM: http://git.debian.org/?p=pkg-php/php.git;a=commit;h=d09fd04ed7bfcf7f008360c6a42025108925df09

CONFIRM: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=618489

XF: http://xforce.iss.net/xforce/xfdb/66180

BID: http://www.securityfocus.com/bid/46928

CVE Reference: CVE-2011-0441

- **CVE-2011-1551 Novell CVSS 2.0 Score = 7.2**

SUSE openSUSE Factory assigns ownership of the /var/log/cobbler/ directory tree to the web-service user account, which might allow local users to gain privileges by leveraging access to this account during root filesystem operations by the Cobbler daemon.

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

References:

MLIST: http://openwall.com/lists/oss-security/2011/03/23/11

CVE Reference: CVE-2011-1551

- **CVE-2011-0024 Wireshark CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in wiretap/pcapng.c in Wireshark before 1.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted capture file.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=671331

VUPEN: http://www.vupen.com/english/advisories/2011/0719

REDHAT: http://www.redhat.com/support/errata/RHSA-2011-0370.html

SECUNIA: http://secunia.com/advisories/43821

CVE Reference: CVE-2011-0024

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