

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

Another certificate compromise. New worm using Remote Desktop Protocol. California law requires direct notice to breached residents. Financial Institutions getting better at fast detection of account takeover.

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

• DigiNotar said attack is to blame for certificate compromise

The business responsible for issuing a bogus Google.com SSL certificate revealed Tuesday that its infrastructure was hacked.

The breach permitted the "fraudulent issuance of public key certificates for a number of domains, including Google.com," according to the statement from Illinois-based VASCO, which owns the Dutch-based DigiNotar, a certificate authority (CA).

Once it detected the hack on July 19, DigiNotar revoked all of the counterfeit certificates. But now the company admits that at least one remained live, the statement said. SC Magazine

Full Story :

http://www.scmagazineus.com/diginotar-said-attack-is-to-blame-for-certificate-compromise/article/210891/?utm_source=

• Morto using DNS for command-and-control

Morto, the first-ever worm to spread via Windows Remote Desktop Protocol (RDP), is not only unique because of its propagation mechanism - it also uses a novel vector, domain name system (DNS) records, to communicate with infected machines, a Symantec researcher said Wednesday.

The DNS is a critical component of internet infrastructure that translates IP addresses into memorable domain names, such as SCMagazineUS.com.

Specifically, Morto uses DNS TXT records for its communication protocol, Cathal Mullaney, security response engineer at Symantec, said in a blog post Wednesday. Such records were originally used to allow text to be stored with a DNS record. Nowadays, however, they more often are used to store machine-readable data. SC Magazine

Full Story :

http://www.scmagazineus.com/morto-using-dns-for-command-and-control/article/210962/?utm_source=feedburner&

• California blazes trail again with enhanced breach alert law

After being vetoed twice by the prior administration, a bill that updates California's pioneering data breach notification law was signed into law Wednesday by Gov. Jerry Brown.

Introduced by Democratic state Sen. Joe Simitian, SB-24 bolsters SB-1386, the nation's first law requiring companies to alert California residents if their personal data is accessed illegally. Since that legislation took effect eight years ago, nearly all 50 states have followed suit with their own versions.

The update, meanwhile, requires that breach notification letters contain specifics of the incident, including the type of personal information exposed, a description of what happened, and advice on steps to take to protect oneself from identity theft. The law also mandates that organizations that sustain a breach affecting 500 or more people submit a copy of the alert letter to the state attorney general's office. SC Magazine

Full Story :

http://www.scmagazineus.com/california-blazes-trail-again-with-enhanced-breach-alert-law/article/211005/?utm_source=feedburner&

• Account takeover still common, but getting detected faster

Banks are still getting hit hard by hackers who take over corporate accounts, but financial institutions are doing a better job at spotting the fraud before any money is drained out, according to a new survey.

The report from the Financial Services Information Sharing and Analysis Center (FS-ISAC), released Thursday, polled 77 banks. Twenty-one said their corporate customers were victimized by account seizures, in which cybercriminals gain control of an organization's bank account, usually by stealing login credentials through malware or phishing.

Of the reported takeovers, 86 occurred in 2009, but that number rose to 108 in the first six months of 2010, the survey showed. SC Magazine

Full Story :

http://www.scmagazineus.com/account-takeover-still-common-but-getting-detected-faster/article/210535/?utm_source=feedburner&

• More insiders snooping into health records, says survey

Breaches into protected health information (PHI) are on the rise, and staffers are responsible for more than a third of the intrusions, a new survey has found. The "2011 Survey of Patient Privacy Breaches" from Veriphys, a Los Altos, Calif.-based provider of identity and access intelligence, determined that more than 70 percent of organizations surveyed were targets of one or more breaches of PHI within the last 12 months. And, insiders were responsible for the majority of breaches, with 35 percent taking an unauthorized look at medical data of fellow employees and 27 percent peeking at records of friends and relatives.

The survey, released Wednesday, tabulated responses from 90 compliance and privacy officers at mid- to large-size hospitals and health care service providers who were asked online about their views of privacy and compliance initiatives within their organization, the adequacy of tools used to monitor unauthorized access to PHI, and the number and type of breaches sustained in the past year. SC Magazine

Full Story :

http://www.scmagazineus.com/more-insiders-snooping-into-health-records-says-survey/article/210927/?utm_source=feedburner&

New Vulnerabilities Tested in SecureScout

• 19441 Adobe Flash Player buffer overflow Vulnerability (CVE-2011-2415) (Remote File Checking)

Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130,

CVE-2011-2134, CVE-2011-2137, and CVE-2011-2414.

Adobe Flash Player version 10.3.183.5 resolves the issue.

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

References:

- * BID: 49077
<http://www.securityfocus.com/bid/49077>
- * SECTRACK: 1025907
<http://securitytracker.com/id/1025907>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-21.html>
- * REDHAT: RHSA-2011:1144
<http://www.redhat.com/support/errata/RHSA-2011-1144.html>
- * SUSE: SUSE-SA:2011:033
<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00006.html>

CVE Reference:

CVE-2011-2415 (cve.mitre.org, nvd.nist.gov)

● **19442 Adobe Flash Player integer overflow Vulnerability (CVE-2011-2416) (Remote File Checking)**

Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2136 and CVE-2011-2138.

Adobe Flash Player version 10.3.183.5 resolves the issue.

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

References:

- * BID: 49081
<http://www.securityfocus.com/bid/49081>
- * SECTRACK: 1025907
<http://securitytracker.com/id/1025907>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-21.html>
- * REDHAT: RHSA-2011:1144
<http://www.redhat.com/support/errata/RHSA-2011-1144.html>
- * SUSE: SUSE-SA:2011:033
<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00006.html>

CVE Reference:

CVE-2011-2416 (cve.mitre.org, nvd.nist.gov)

● **19443 Adobe Flash Player memory corruption Vulnerability (CVE-2011-2417) (Remote File Checking)**

Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2140, and CVE-2011-2425.

Adobe Flash Player version 10.3.183.5 resolves the issue.

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

References:

- * BID: 49084
<http://www.securityfocus.com/bid/49084>
- * SECTRACK: 1025907
<http://securitytracker.com/id/1025907>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-21.html>
- * REDHAT: RHSA-2011:1144
<http://www.redhat.com/support/errata/RHSA-2011-1144.html>
- * SUSE: SUSE-SA:2011:033

<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00006.html>

CVE Reference:

CVE-2011-2417 (cve.mitre.org, nvd.nist.gov)

• **19444 Adobe Flash Player memory corruption Vulnerability (CVE-2011-2425) (Remote File Checking)**

Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2140, and CVE-2011-2417.

Adobe Flash Player version 10.3.183.5 resolves the issue.

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

References:

- * BID: 49085
<http://www.securityfocus.com/bid/49085>
- * SECTRACK: 1025907
<http://securitytracker.com/id/1025907>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-21.html>
- * REDHAT: RHSA-2011:1144
<http://www.redhat.com/support/errata/RHSA-2011-1144.html>
- * SUSE: SUSE-SA:2011:033
<http://lists.opensuse.org/opensuse-security-announce/2011-08/msg00006.html>

CVE Reference:

CVE-2011-2425 (cve.mitre.org, nvd.nist.gov)

• **19445 Adobe Flash Player multiple memory corruption Vulnerabilities (CVE-2011-2424) (Remote File Checking)**

Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted SWF file, as demonstrated by "about 400 unique crash signatures."

Adobe Flash Player version 10.3.183.5 resolves the issue.

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

References:

- * BID: 49186
<http://www.securityfocus.com/bid/49186>
- * SECTRACK: 1025907
<http://securitytracker.com/id/1025907>
- * MISC:
<http://googleonlinesecurity.blogspot.com/2011/08/fuzzing-at-scale.html>
- * MISC:
<http://twitter.com/taviso/statuses/101046246277521409>
- * MISC:
<http://twitter.com/taviso/statuses/101046396790128640>
- * CONFIRM:
<http://blogs.adobe.com/asset/2011/08/how-did-you-get-to-that-number.html>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-21.html>
- * REDHAT: RHSA-2011:1144
<http://www.redhat.com/support/errata/RHSA-2011-1144.html>

CVE Reference:

CVE-2011-2424 (cve.mitre.org, nvd.nist.gov)

• **19446 Wireshark malformed X.509if packet denial of service Vulnerability (Remote File Checking)**

The X.509if dissector in Wireshark 1.2.x before 1.2.16 and 1.4.x before 1.4.5 does not properly initialize certain global variables, which allows remote attackers to cause a denial of service (application crash) via a crafted .pcap file.

The vulnerability has been addressed in versions 1.2.16 and 1.4.5.

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

References:

- * MLIST: [oss-security] 20110418 Re: Wireshark 1.2.16 / 1.4.5
<http://openwall.com/lists/oss-security/2011/04/18/8>
- * MLIST: [oss-security] 20110418 Wireshark 1.2.16 / 1.4.5
<http://openwall.com/lists/oss-security/2011/04/18/2>
- * CONFIRM:
<http://anonsvn.wireshark.org/viewvc?revision=36608&view=revision>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2011-05.html>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2011-06.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5754
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5793
- * FEDORA: FEDORA-2011-5529
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/058993.html>
- * FEDORA: FEDORA-2011-5569
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/058983.html>
- * FEDORA: FEDORA-2011-5621
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/058900.html>
- * OSVDB: 71846
<http://www.osvdb.org/71846>
- * SECTRACK: 1025388
<http://securitytracker.com/id?1025388>
- * SECUNIA: 44172
<http://secunia.com/advisories/44172>
- * SECUNIA: 44374
<http://secunia.com/advisories/44374>
- * VUPEN: ADV-2011-1022
<http://www.vupen.com/english/advisories/2011/1022>
- * VUPEN: ADV-2011-1106
<http://www.vupen.com/english/advisories/2011/1106>
- * BID: 47392
<http://www.securityfocus.com/bid/47392>

CVE Reference:

CVE-2011-1590 (cve.mitre.org, nvd.nist.gov)

• 19447 Wireshark NFS dissector denial of service Vulnerability (Remote File Checking)

The NFS dissector in epan/dissectors/packet-nfs.c in Wireshark 1.4.x before 1.4.5 on Windows uses an incorrect integer data type during decoding of SETCLIENTID calls, which allows remote attackers to cause a denial of service (application crash) via a crafted .pcap file.

The vulnerability has been addressed in versions 1.4.5.

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

References:

- * BID: 47392
<http://www.securityfocus.com/bid/47392>
- * MLIST: [oss-security] 20110418 Re: Wireshark 1.2.16 / 1.4.5
<http://openwall.com/lists/oss-security/2011/04/18/8>
- * MLIST: [oss-security] 20110418 Wireshark 1.2.16 / 1.4.5
<http://openwall.com/lists/oss-security/2011/04/18/2>
- * CONFIRM:
<http://anonsvn.wireshark.org/viewvc?revision=34115&view=revision>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2011-06.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5209
- * OSVDB: 71847
<http://www.osvdb.org/71847>
- * SECUNIA: 44172

<http://secunia.com/advisories/44172>

* VUPEN: ADV-2011-1022

<http://www.vupen.com/english/advisories/2011/1022>

* XF: wireshark-nfs-dos(66833)

<http://xforce.iss.net/xforce/xfdb/66833>

CVE Reference:

CVE-2011-1592 (cve.mitre.org, nvd.nist.gov)

• 19448 Wireshark DECT dissector buffer overflow Vulnerability (Remote File Checking)

Stack-based buffer overflow in the DECT dissector in epan/dissectors/packet-dect.c in Wireshark 1.4.x before 1.4.5 allows remote attackers to execute arbitrary code via a crafted .pcap file.

The vulnerability has been addressed in versions 1.4.5.

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

References:

* BID: 47392

<http://www.securityfocus.com/bid/47392>

* EXPLOIT-DB: 17185

<http://www.exploit-db.com/exploits/17185>

* EXPLOIT-DB: 17195

<http://www.exploit-db.com/exploits/17195>

* MLIST: [oss-security] 20110418 Re: Wireshark 1.2.16 / 1.4.5

<http://openwall.com/lists/oss-security/2011/04/18/8>

* MLIST: [oss-security] 20110418 Wireshark 1.2.16 / 1.4.5

<http://openwall.com/lists/oss-security/2011/04/18/2>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2011-06.html>

* CONFIRM:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5836

* CONFIRM:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5838

* FEDORA: FEDORA-2011-5529

<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/058993.html>

* FEDORA: FEDORA-2011-5569

<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/058983.html>

* FEDORA: FEDORA-2011-5621

<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/058900.html>

* CERT-VN: VU#243670

<http://www.kb.cert.org/vuls/id/243670>

* OSVDB: 71848

<http://www.osvdb.org/71848>

* SECTRACK: 1025389

<http://securitytracker.com/id?1025389>

* SECUNIA: 44172

<http://secunia.com/advisories/44172>

* SECUNIA: 44374

<http://secunia.com/advisories/44374>

* VUPEN: ADV-2011-1022

<http://www.vupen.com/english/advisories/2011/1022>

* VUPEN: ADV-2011-1106

<http://www.vupen.com/english/advisories/2011/1106>

* XF: wireshark-dect-bo(66834)

<http://xforce.iss.net/xforce/xfdb/66834>

CVE Reference:

CVE-2011-1591 (cve.mitre.org, nvd.nist.gov)

• 19449 Wireshark DICOM dissector denial of service Vulnerability (Remote File Checking)

The dissect_dcm_main function in epan/dissectors/packet-dcm.c in the DICOM dissector in Wireshark 1.2.x before 1.2.17 and 1.4.x before 1.4.7 allows remote attackers to cause a denial of service (infinite loop) via an invalid PDU length.

The vulnerability has been addressed in versions 1.2.17, and 1.4.7.

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

References:

- * MLIST: [oss-security] 20110531 CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues <http://openwall.com/lists/oss-security/2011/05/31/20>
- * MLIST: [oss-security] 20110601 Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues <http://openwall.com/lists/oss-security/2011/06/01/1>
- * MLIST: [oss-security] 20110601 Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues <http://openwall.com/lists/oss-security/2011/06/01/11>
- * CONFIRM: <http://anonsvn.wireshark.org/viewvc?view=revision&revision=36958>
- * CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2011-07.html>
- * CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2011-08.html>
- * CONFIRM: https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5876
- * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=710021
- * BID: 48066 <http://www.securityfocus.com/bid/48066>
- * SECUNIA: 44449 <http://secunia.com/advisories/44449>

CVE Reference:

CVE-2011-1957 (cve.mitre.org, nvd.nist.gov)

• 19450 Wireshark Diameter dictionary file denial of service Vulnerability (Remote File Checking)

Wireshark 1.2.x before 1.2.17 and 1.4.x before 1.4.7 allows user-assisted remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Diameter dictionary file.

The vulnerability has been addressed in versions 1.2.17, and 1.4.7.

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

References:

- * MLIST: [oss-security] 20110531 CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues <http://openwall.com/lists/oss-security/2011/05/31/20>
- * MLIST: [oss-security] 20110601 Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues <http://openwall.com/lists/oss-security/2011/06/01/1>
- * MLIST: [oss-security] 20110601 Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues <http://openwall.com/lists/oss-security/2011/06/01/11>
- * CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2011-07.html>
- * CONFIRM: <http://www.wireshark.org/security/wnpa-sec-2011-08.html>
- * CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=710184
- * BID: 48066 <http://www.securityfocus.com/bid/48066>
- * SECUNIA: 44449 <http://secunia.com/advisories/44449>

CVE Reference:

CVE-2011-1958 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-3192 Apache CVSS 2.0 Score = 7.8

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

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

References:

MLIST:

http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/%3cCAAPSnn2PO-d-C4nQt_TES2RRWiZr7urefhTKP

CONFIRM: https://issues.apache.org/bugzilla/show_bug.cgi?id=51714

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=732928

CONFIRM: <http://www.gossamer-threads.com/lists/apache/dev/401638>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/17696>

SECTRAK: <http://securitytracker.com/id?1025960>

SECUNIA: <http://secunia.com/advisories/45606>

FULLDISC: <http://seclists.org/fulldisclosure/2011/Aug/175>

MLIST:

http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3c20110824161640.122D387DD@minotaur.a

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0285.html>

CVE Reference: [CVE-2011-3192](#)

• **CVE-2011-3190 Apache CVSS 2.0 Score = 7.5**

Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.33, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request.

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

References:

MISC: https://issues.apache.org/bugzilla/show_bug.cgi?id=51698

XF: <http://xforce.iss.net/xforce/xfdb/69472>

SECTRAK: <http://www.securitytracker.com/id?1025993>

BID: <http://www.securityfocus.com/bid/49353>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/519466/100/0/threaded>

SECUNIA: <http://secunia.com/advisories/45748>

CVE Reference: [CVE-2011-3190](#)

• **CVE-2011-2712 Apache CVSS 2.0 Score = 2.6**

Cross-site scripting (XSS) vulnerability in Apache Wicket 1.4.x before 1.4.18, when setAutomaticMultiWindowSupport is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

XF: <http://xforce.iss.net/xforce/xfdb/69394>

BID: <http://www.securityfocus.com/bid/49290>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/519398/100/0/threaded>

CONFIRM: <http://wicket.apache.org/2011/08/23/cve-2011-2712.html>

SECUNIA: <http://secunia.com/advisories/45727>

CVE Reference: [CVE-2011-2712](#)

• **CVE-2011-2555 Cisco CVSS 2.0 Score = 10.0**

Cisco TelePresence Recording Server 1.7.2.x before 1.7.2.1 has a default password for the root administrator account, which makes it easier for remote attackers to modify the configuration via an SSH session, aka Bug ID CSCtr76182.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/68887>

BID: <http://www.securityfocus.com/bid/48932>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b8ad3f.shtml

SECTRAK: <http://securitytracker.com/id?1025872>

CVE Reference: [CVE-2011-2555](#)

• **CVE-2011-1643 Cisco CVSS 2.0 Score = 10.0**

Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 6.x, 7.x before 7.1(5b)su4, 8.0, and 8.5 before 8.5(1)su2 and Cisco Unified Presence Server 6.x, 7.x, 8.0, and 8.5 before 8.5xnr allow remote attackers to read database data by connecting to a query interface through an SSL session, aka Bug IDs CSCti81574, CSCto63060, CSCto72183, and CSCto73833.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b8f532.shtml

CVE Reference: [CVE-2011-1643](#)

• **CVE-2011-3268 PHP CVSS 2.0 Score = 10.0**

Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.

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

References:

BID: <http://www.securityfocus.com/bid/49241>

CONFIRM: <http://www.php.net/ChangeLog-5.php#5.3.7>

CONFIRM: <http://www.php.net/archive/2011.php#id2011-08-18-1>

CVE Reference: [CVE-2011-3268](#)

• **CVE-2011-2564 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the Service Advertisement Framework (SAF) in Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 8.x before 8.5(1) and Cisco Intercompany Media Engine 8.x before 8.5(1) allows remote attackers to cause a denial of service (device reload) via crafted SAF packets, aka Bug ID CSCth19417.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b8f533.shtml

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b8f531.shtml

CVE Reference: [CVE-2011-2564](#)

• **CVE-2011-2563 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the Service Advertisement Framework (SAF) in Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 8.x before 8.5(1) and Cisco Intercompany Media Engine 8.x before 8.5(1) allows remote attackers to cause a denial of service (device reload) via crafted SAF packets, aka Bug ID CSCth26669.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b8f533.shtml

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b8f531.shtml

CVE Reference: [CVE-2011-2563](#)

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