**ScoutNews Team** **December 2, 2005**
**Issue # 48**

Weekly ScoutNews by netVigilance

**Table of Contents**



## This Week in Review

SONY's silence adds to negative press along with DRM's own copyright violations, Scottrade unwittingly shares Social Security numbers, Phishing report: Sharks are cleaning up and Dr. Chaos goes the way of Dr. No.

Enjoy reading and 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

- **SONY on how not to conduct a PR campaign**

Business Week jumps on the SONY negative press bandwagon and a 5000+ signature grass-roots rebellion posted on the website **PetitionOnline.com**.

Sources are pointing to the initial silence about the existence of the spyware further bruised their image. The Finnish security company F-Secure alerted SONY roughly one month before the incident blew up and hit the press. With PR like this who needs enemies?

BusinessWeek

Related Links:

http://www.businessweek.com/technology/content/nov2005/tc20051129_938966.htm

http://www.businessweek.com/technology/content/dec2005/tc20051202_241333.htm?campaign_id=topStories_ssi_5

### ❖ SONY DRM software may have violated open-source copyright

This just keeps getting better - Matti Nikki and Sebastian Porst have uncovered the strong likelihood that the Sony/First4Internet XCP copy protection software itself infringes several copyrights.

They claim that the code file ECDPlayerControl.ocx, which ships as part of XCP, contains code from several copyrighted programs, including LAME, id3lib, mpglib, mpg123, FAAC, and most amusingly, DVD-Jon's DRMS. These are all open-source programs that are protected under GPL licensing.

Freedom-to-tinker

Full Story :
http://www.freedom-to-tinker.com/?p=933

### ❖ Scottrade gets breached, millions of records compromised

The St. Louis based online trading house announced this week that it was victim to a hacker attack that may have compromised the SSN and brokerage account records of some 1.3 Million customers.

Scottrade advised customers to 'seriously consider' placing a fraud alert on their credit files.

Source

Related Links:
http://www.tgdaily.com/2005/11/28/scottrade-hackersgainaccess/

### ❖ Email phising exploits snaring big catches

'Tis the season to bait users with promises of quick cash. A sophisticated phising scam is circulating with promises of an IRS refund. This attack is very insidious since the message asks the user to copy / paste the IRS website into their browser address bar for safety; but via cross-site scripting (XSS), the victim is actually re-directed to a bogus site.

Another Phishing exploit lures users in with the promise of money from a fictitious PayPal class action lawsuit. All you have to do is update your PayPal account information regarding your bank account and credit card data.

Related Links:
http://antivirus.about.com/od/emailscams/a/irsphishing.htm
http://www.malwarehelp.org/news/View.php?ArticleID=1292

- **Dr. Chaos ends his mayhem**

"World domination; the same old dream. Our asylums are full of people who think they're Napoleon, or God." – *Ian Fleming (James Bond)*

The hacker who called himself "Dr. Chaos" was sentenced to seven years in prison for his involvement in causing power failures in the Midwest U.S. by hacking into power company computers.

The evil Doctor apparently headed a hacker group that called themselves the "Realm of Chaos". ( Looks like his realm is now a 10'x10' cell – *Ed.*)

Full Story:
http://www.phillyburbs.com/pb-dyn/news/1-11302005-577691.html

# New Vulnerabilities Tested in SecureScout

- **17680 Bugzilla "config.cgi" script Information Disclosure Vulnerability**

  Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

  The problem is that it is possible to access the "config.cgi" script without being authenticated even when the "requirelogin" parameter setting is enabled. This can be exploited to disclose certain product information (e.g. product names).

  The security issue has been reported in versions 2.18rc1 through 2.18.3, 2.19 through 2.20rc2, and 2.21.

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

  **References:**

  Original advisory:
  http://www.bugzilla.org/security/2.18.4/

  Other references:

http://secunia.com/advisories/17030/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** None

### ❖ 17714 Bugzilla "usevisibilitygroups" parameter Information Disclosure Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

The problem is that it is possible to list invisible users when using the user matching feature when the "usevisibilitygroups" parameter setting is enabled.

Successful exploitation requires that user matching is enabled in "substring" mode.

The security issue has been reported in versions 2.19.1 through 2.20rc2, and 2.21.

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

**References:** Original advisory:
http://www.bugzilla.org/security/2.18.4/

Other references:
http://secunia.com/advisories/17030/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** None

### ❖ 17715 Bugzilla process_bug.cgi script Information Disclosure Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

Input passed to process_bug.cgi is not properly verified before being used. This makes it possible to change a flag on a bug report that the user does not have access to, and can be exploited to email the bug summary to the malicious user.

The vulnerability affects versions 2.17.1 through 2.18.1, and development snapshots 2.19.1 through 2.19.3.

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

**References:**

Original advisory:
http://www.bugzilla.org/security/2.18.1/
https://bugzilla.mozilla.org/show_bug.cgi?id=293159
https://bugzilla.mozilla.org/show_bug.cgi?id=292544

Other references:
http://secunia.com/advisories/16021/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** CAN-2005-2173, CAN-2005-2174

### ❖ 17716 Bugzilla bug report as private view the report Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

A race condition when marking a bug report as private in the database can be exploited to view the report when there is a MySQL replication lag.

The vulnerability affects versions 2.17.1 and above.

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

**References:**

Original advisory:
http://www.bugzilla.org/security/2.18.1/
https://bugzilla.mozilla.org/show_bug.cgi?id=293159
https://bugzilla.mozilla.org/show_bug.cgi?id=292544

Other references:
http://secunia.com/advisories/16021/

Product HomePage:
http://www.bugzilla.org

**CVE Reference:** CAN-2005-2173, CAN-2005-2174

### ❖ 17717 Bugzilla invisible product Information Disclosure Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

Users can determine whether or not a given invisible product exists, as an access denied error is returned when the user attempts to access a valid product.

Users can also enter bugs into products closed for bug entry, if a valid product name is known.

This weakness affects versions 2.10 through 2.18, 2.19.1, and 2.19.2

Test Case Impact: **Gather Info.** Vulnerability Impact: **Low** Risk: **Gather Info.**

**References:**

Original advisory:
http://www.bugzilla.org/security/2.16.8/
https://bugzilla.mozilla.org/show_bug.cgi?id=287109
https://bugzilla.mozilla.org/show_bug.cgi?id=287436

Other references:
http://secunia.com/advisories/15338/

Product HomePage:
http://www.bugzilla.org

**CVE Reference:** CAN-2005-1563, CAN-2005-1564, CAN-2005-1565

### ❖ 17718 Bugzilla user's password visible in logs Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

A user's password may be embedded as part of a report URL, which causes it to be visible in the web logs.

This weakness affects versions 2.17.1 through 2.18, 2.19.1, and 2.19.2

Test Case Impact: **Gather Info.** Vulnerability Impact: **Low** Risk: **Gather Info.**

**References:**

Original advisory:
http://www.bugzilla.org/security/2.16.8/
https://bugzilla.mozilla.org/show_bug.cgi?id=287109
https://bugzilla.mozilla.org/show_bug.cgi?id=287436

Other references:
http://secunia.com/advisories/15338/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** CAN-2005-1563, CAN-2005-1564, CAN-2005-1565

### ❖ 17719 Bugzilla Internal Error Response Cross-Site Scripting Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users

to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

Michael Krax has reported a vulnerability in Bugzilla, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed in HTTP requests is not properly sanitized before being returned to users in error messages when an internal error is encountered. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

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

**References:**

Original advisory:
http://www.bugzilla.org/security/2.16.7-nr/
https://bugzilla.mozilla.org/show_bug.cgi?id=272620

Other references:
http://secunia.com/advisories/13701/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** CAN-2004-1061

### ❖ 17720 Bugzilla "process_bug.cgi" script remove keywords Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

An error in "process_bug.cgi" can be exploited via a specially crafted HTTP POST request to remove keywords from a bug, even though the user doesn't have "edigbugs" permissions.

The issue affects versions 2.9 through 2.18rc2 and 2.19.

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

**References:**

Original advisory:
http://www.bugzilla.org/security/2.16.6/

Other references:
http://secunia.com/advisories/12939/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** None

### ❖ 17721 Bugzilla exporting bugs to XML Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

An error when exporting bugs to XML exposes user comments and attachment summaries marked as private to users, who are not members of the group allowed to see the comments.

Successful exploitation requires that the "insidergroup" feature is used.

The issue affects versions 2.17.1 through 2.18rc2 and 2.19.

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

**References:**

Original advisory:
http://www.bugzilla.org/security/2.16.6/

Other references:
http://secunia.com/advisories/12939/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** None

### ❖ 17722 Bugzilla private attachment metadata Information Disclosure Vulnerability

Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

Changes of various private attachment metadata (filename, description, MIME type, and review flags) are disclosed to users, who are not members of the group allowed to see private attachments.

Successful exploitation requires that the "insidergroup" feature is used.

The issue affects versions 2.17.1 through 2.18rc2 and 2.19.

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

**References:**

Original advisory:
http://www.bugzilla.org/security/2.16.6/

Other references:
http://secunia.com/advisories/12939/

Product HomePage:
http://www.bugzilla.org/

**CVE Reference:** None

# New Vulnerabilities found this Week

**Avaya Media Gateway IP Media Resource 320 Denial of Service**
"Denial of Service"

A vulnerability has been reported in Avaya Media Gateway TN2602AP IP Media Resource 320, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error. This can be exploited to cause memory leaks, which can potentially cause a DoS via specially crafted packets.

The vulnerability has been reported in all firmware versions prior to vintage 9.

Note: TN2602AP IP Media Resource 320 circuit pack is an optional component of Avaya G650 Media Gateway.

References:
http://support.avaya.com/elmodocs2/security/ASA-2005-231.pdf

**Cisco Security Agent Local Privilege Escalation Vulnerability**
"Gain escalated privileges"

A vulnerability has been reported in Cisco Security Agent (CSA), which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error in CSA on the Windows platform. This can be exploited by malicious users to gain SYSTEM privileges on a vulnerable system.

The vulnerability has been reported in the following versions:
* Cisco CSA version 4.5.0 (all builds) managed and standalone agents.
* Cisco CSA version 4.5.1 (all builds) managed and standalone agents.
* Cisco CSA version 4.5.0 (build 573) for CallManager.
* Cisco CSA version 4.5.1 (build 628) for CallManager.
* Cisco CSA version 4.5.1 (build 616) for Intelligent Contact Management (ICM), IPCC Enterprise, and IPCC Hosted.
* Cisco CSA version 4.5.0 ( build 573) for Cisco Voice Portal (CVP) 3.0 and 3.1.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20051129-csa.shtml

**Mac OS X Security Update Fixes Multiple Vulnerabilities**
"Bypass certain security restrictions; compromise a user's system"

Apple has issued a security update for Mac OS X, which fixes 13 vulnerabilities.

1) An error in the handling of HTTP headers in the Apache 2 web server can be exploited by malicious people to conduct HTTP request smuggling attacks when Apache is used in conjunction with certain proxy servers, caching servers, or web application firewalls.

2) An error in the Apache web server's "mod_ssl" module may be exploited by malicious people to bypass certain security restrictions.

3) A boundary error exists in CoreFoundation when resolving certain URL. This can be exploited to cause a heap-based buffer overflow and may allow arbitrary code execution via a specially-crafted URL. CoreFoundation is used by Safari and other applications.

4) An error in curl when handling NTLM authentication can be exploited by malicious people to compromise a user's system.

5) An error exists in the ODBC Administrator utility helper tool "iodbcadmintoo". This can be exploited by malicious, local users to execute commands with escalated privileges.

6) An error in OpenSSL when handling certain compatibility options can potentially be exploited by malicious people to perform protocol rollback attacks.

7) An error in the passwordserver when handling the creation of an Open Directory master server may cause certain credentials to be disclosed. This can be exploited by unprivileged local users to gain elevated privileges on the server.

8) An integer overflow error exists in the PCRE library that is used by Safari's JavaScript engine. This can potentially be exploited by malicious people to compromise a user's system.

9) An error exists in Safari when saving a downloaded file with an overly long filename. This can be exploited to cause the download file to be saved outside of the designated download directory.

10) JavaScript dialog boxes in Safari do not indicate the web site that created them. This can be exploited by malicious web sites to spoof dialog boxes.

11) A boundary error exists in WebKit when handling certain specially crafted content. This can be exploited to cause a heap-based buffer overflow via content downloaded from malicious web sites in applications that use WebKit such as Safari.

12) An error in sudo can be exploited by malicious, local users to execute arbitrary commands with escalated privileges.

13) The syslog server does not properly sanitise messages before recording them.

This can be exploited to forge log entries and mislead the system administrator by supplying messages certaining control characters, such as the newline character, to the syslog server.

References:
http://docs.info.apple.com/article.html?artnum=302847

**Linux Kernel Multiple Denial of Service Vulnerabilities**
"Denial of Service"

Some vulnerabilities have been reported in the Linux Kernel, which potentially can be exploited by malicious, local users to cause a DoS (Denial of Service).

1) An error in the auto-reap of child processes that have ptrace attached can lead to dangling ptrace references. This may be exploited by local users to cause a kernel crash.

2) The use of "printk()" in the "time_out_leases()" function in "/fs/locks.c" can consume a large amount of kernel log space. This can be exploited by local users to cause a DoS by generating a large number of broken leases.

The vulnerabilities have been reported in the 2.6 kernel branch.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.15-rc3

**Cisco IOS HTTP Server Script Insertion Vulnerability**
"Conduct script insertion attacks"

Hugo Vazquez Carames has reported a vulnerability in Cisco IOS, which can be exploited by malicious people to conduct script insertion attacks.

The vulnerability is caused due to the memory dump feature of the HTTP server not properly sanitising the data in received packets before displaying them to the user in a HTML formatted page when the user views the "/level/15/exec/-/buffers/assigned/dump" link. This can be exploited to execute arbitrary script code in a user's browser session when the user views a memory dump containing malicious Javascript/HTML code from a received packet.

Successful exploitation may allow the attacker to perform certain actions that are accessible by the logon administrator. E.g. changing the "enable" password by injecting HTML code that requests for the "/level/15/configure/-/enable/secret/" link.

References:
http://www.infohacking.com/INFOHACKING_RESEARCH/Our_Advisories/cisco/index.html

**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