netVigilance

ScoutNews Team **December 9, 2005**
Issue # 49

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Digital cameras employed in data thievery, some Arabic news agency gets spear-phished and Clunk-B Trojan spotted.

Enjoy reading.

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

❖ Hackers employ digital cameras to steal data

'Camsnuffling', the latest hackers moniker; involves hackers using digital cameras to extract and store data.

This new threat represents yet another information port to monitor in the war against electronic intrusion.

Ian Callens, Icomm Technologies, explains: "This is a very difficult issue to manage and a real threat to business continuity and data security. If someone is seen in the workplace using an iPod it's more than likely that it's for the wrong reasons – either podslurping or downloading music without permission. This is relatively easier to police."

IT Observer

Related Links:
http://www.ebcvg.com/articles.php?id=966

❖ Arabic news agency hit by spear phishing

"a prominent Arab media outlet" was the target of a spear-Phishing attack this week. Specific users at the unnamed new agency were targeted with emails promising unreleased pictures of Osama-Bin-Laden. So-called spear phishing differs from standard phishing attacks in that it targets a very specific group of people, somewhat like social engineering.

vnunet.com

Related Links:
http://www.vnunet.com/vnunet/news/2147197/arabic-news-station-hit

❖ Clunky-B Trojan on the loose

Sophos has reported a vulnerability in IE being exploited by the Clunk-B Trojan. Clunky-B could be used to download malicious code or viruses to the unsuspecting visitors to infected sites.

The attackers have used emails to coax users into clicking through to infected websites. Make sure you have anti-virus signatures up-to-date and IE patches installed.
PCPro

Full Story:
http://www.pcpro.co.uk/news/81004/clunkyb-exploits-unpatched-ie-vuln.html

New Vulnerabilities Tested in SecureScout

❖ 17723 Bugzilla error message disclosing the database password 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.

Under certain circumstances, an error message disclosing the database password is returned when the SQL server is stopped, and the web server is still running.

This security issue affects versions 2.17.1 through 2.17.7.

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

References:

Original advisory:

http://www.bugzilla.org/security/2.16.5/

Other references:
http://secunia.com/advisories/12057/

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

CVE Reference: None

❖ 17724 Bugzilla grant membership 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 privileged user able to grant membership to some groups (usually administrators) can bypass the administrative controls and grant membership to groups other than the ones, which the user has privileges for.

This vulnerability affects versions 2.17.1 through 2.17.7.

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

References:

Original advisory:
http://www.bugzilla.org/security/2.16.5/

Other references:
http://secunia.com/advisories/12057/

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

CVE Reference: None

❖ 17725 Bugzilla "duplicates.cgi" and "buglist.cgi" CGI scripts 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.

When Bugzilla is configured to hide certain products from users, it is still possible to gain knowledge of the names of these products via the "duplicates.cgi" and "buglist.cgi" CGI scripts.

This issue affects all versions prior to 2.16.6 and 2.18rc1.

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

References:

Original advisory:
http://www.bugzilla.org/security/2.16.5/

Other references:
http://secunia.com/advisories/12057/

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

CVE Reference: None

❖ 17726 Bugzilla Input passed to several administration CGI scripts not properly sanitised 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 several administration CGI scripts is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a administrative user's browser session in context of an affected site.

The following CGI scripts are vulnerable:
* editcomponents.cgi
* editgroups.cgi
* editmilestones.cgi
* editproducts.cgi
* editusers.cgi
* editversions.cgi

This vulnerability affects all versions prior to 2.16.6 and 2.18rc1.

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

References:

Original advisory:
http://www.bugzilla.org/security/2.16.5/

Other references:
http://secunia.com/advisories/12057/

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

CVE Reference: None

❖ 17727 Bugzilla user's login ID and password included as part of the image URL 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.

When a user is prompted to login when attempting to view a chart, the user's login ID and password are included as part of the image URL. This may disclose the information in web server log files.

This security issue affects versions 2.17.5 through 2.17.7.

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

References:

Original advisory:
http://www.bugzilla.org/security/2.16.5/

Other references:
http://secunia.com/advisories/12057/

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

CVE Reference: None

❖ 17728 Bugzilla input validation error in "editusers.cgi" 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 input validation error in "editusers.cgi" can be exploited by a malicious, privileged user to manipulate SQL queries by injecting arbitrary SQL code into the "query" parameter.

Successful exploitation requires that the user has privileges to grant membership to any group (usually administrators).

This vulnerability affects all versions prior to 2.16.6 and 2.18rc1.

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

References:

Original advisory:
http://www.bugzilla.org/security/2.16.5/

Other references:
http://secunia.com/advisories/12057/

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

CVE Reference: None

❖ 17729 Bugzilla 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.

A vulnerability has been reported in Bugzilla development version 2.17.5, which can be exploited by malicious users to gain access to unprivileged access to restricted data.

The vulnerability is caused due to an information disclosure error in a new feature introduced in version 2.17.5, which allows remote sites to obtain information from Bugzilla. However, this might be exploited to obtain a Bugzilla user's bug information by tricking the user into visiting a malicious website with the new functionality implemented.

This vulnerability affects version 2.17.5.

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

References:

Original advisory:
http://secunia.com/advisories/10199/

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

CVE Reference: None

❖ 17730 Bugzilla "editproducts" privileges 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 with "editproducts" privileges can select arbitrary SQL queries, which will be executed by the cron job "collectstat.pl".

The vulnerability has been reported in various versions prior to 2.17.5 and 2.16.4.

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

References:

Original advisory:
http://bugzilla.mozilla.org/show_bug.cgi?id=214290

Other references:
http://secunia.com/advisories/10149/

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

CVE Reference: None

❖ 17731 Bugzilla "editkeywords" privileges 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 with "editkeywords" privileges can inject arbitrary SQL queries through the URL used to edit existing keywords.

The vulnerability has been reported in various versions prior to 2.17.5 and 2.16.4.

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

References:

Original advisory:
http://bugzilla.mozilla.org/show_bug.cgi?id=219044

Other references:
http://secunia.com/advisories/10149/

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

CVE Reference: None

❖ 17732 Bugzilla Bug group memberships 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.

Bug group memberships aren't properly deleted when a group is deleted. This allows previous members of that group to conduct administrative functions when a new group with the same ID is created.

The vulnerability has been reported in various versions prior to 2.17.5 and 2.16.4.

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

References:

Original advisory:
http://bugzilla.mozilla.org/show_bug.cgi?id=219690

Other references:
http://secunia.com/advisories/10149/

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

CVE Reference: None

New Vulnerabilities found this Week

Microsoft Internet Explorer CSS Import Disclosure of Sensitive Information
“Disclose potentially sensitive information”

Matan Gillon has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to disclose potentially sensitive information.

The vulnerability is caused due to an error where the content of imported CSS (Cascading Style Sheets) from other domains is not properly protected from being read via the "cssText" DHTML property.

This can be exploited by a malicious web site to disclose parts of the content of certain documents served from another web site (e.g. HTML documents with a certain structure which can be parsed by the internal CSS parser), by loading the document via the "@import" directive and accessing the content of it via JavaScript.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2.

References:
http://www.hacker.co.il/security/ie/css_import.html

Sony SunnComm MediaMax DRM Software Insecure Directory Permissions
“Gain escalated privileges”

Jesse Burns and Alex Stamos has reported a security issue in SunnComm MediaMax, which can be exploited by malicious, local users to gain escalated privileges.

The security issue is caused due to insecure default directory ACLs being set on the "SunnComm Shared" directory, which allows "everyone" full access to the directory. This can be exploited by non-administrative users to modify the installed files, and potentially gain escalated privileges by e.g. replacing the MMX.exe program with a malicious program. The MMX.exe program will be automatically executed when another user inserts a MediaMax protected CD.

Changing the directory ACL manually is reportedly not effective as the insecure permissions will be restored the next time a MediaMax protected CD is played.

The security issue has been reported in version 5.0.21.0. Prior versions may also be affected.

References:
http://sonybmg.com/mediamax/

http://www.sonybmg.com/mediamax/titles.html
http://www.eff.org/news/archives/2005_12.php#004234
http://www.eff.org/IP/DRM/Sony-BMG/MediaMaxVulnerabilityReport.pdf

Mozilla Firefox History Information Denial of Service Weakness
"Denial of Service"

ZIPLOCK has discovered a weakness in Mozilla Firefox, which can be exploited by malicious people to cause a DoS (Denial of Service).

The weakness is caused due to an error in the handling of large history information. This can be exploited to fill the history file "history.dat" with large history information by tricking a user into visiting a malicious web site with an overly large title (e.g. set via JavaScript).

Successful exploitation causes the browser to consume a large amount of CPU and memory resources on a vulnerable system when the affected browser is started up again after an attack. Users may have to remove the "history.dat" file in order to be able to use the affected browser.

The weakness has been confirmed in version 1.5. Other versions may also be affected.

References:
http://secunia.com/advisories/17934/

Check Point VPN-1 SecureClient Secure Configuration Verification Bypass Weakness
"Bypass certain security restrictions"

Viktor Steinmann has reported a weakness in Check Point VPN-1 SecureClient, which potentially can be exploited by malicious users to bypass certain security restrictions.

The weakness is caused due to SecureClient relying on the local copy of the "local.scv" file downloaded from the policy server to perform client integrity checks before allowing the client to connect to the internal networks via VPN. This check may be bypassed by users with write-access to the file by continuously replacing it with a modified copy.

This weakness can potentially allow the SCV (Secure Configuration Verification) feature of the product to be bypassed, which allow client systems that are not compliant to the organisation's security policies to connect to the internal networks.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/039634.html

Sun Java System Application Server Reverse SSL Proxy Plug-in Vulnerability
"Man-in-the-Middle"

A vulnerability has been reported in Sun ONE and Java System Application Server, which potentially can be exploited by malicious people to conduct MitM (Man-in-the-Middle) attacks.

The vulnerability is caused due to an unspecified error in the Proxy Plug-in for Sun ONE and Java System Application Server when the plug-in is used with a web server. This may be exploited to conduct MitM (Man-in-the-Middle) attacks. It is reportedly possible to exploit this vulnerability from outside the firewall, although it will be difficult.

The vulnerability has been reported in the following products:
* Sun ONE Application Server 7.
* Sun Java System Application Server Standard Edition 7 2004Q2.
* Sun Java System Application Server Enterprise Edition 8.1 2005Q1.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102012-1

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