



Bill Jones <iudicium@insecurity.org>

[securityalerts] New vulnerabilities found in Moodle 1.6, 1.7, 1.8 and 1.9

1 message

martin@moodle.com <martin@moodle.com>

Fri, Jul 11, 2008 at 4:45 AM

To: securityalerts@lists.moodle.org

Hello,

You are receiving this email because you registered your Moodle site with moodle.org and at that time asked to receive advance security alerts.

A number of security issues in Moodle have been detected and fixed over the past few months. Full details are below. This information will not be published on <http://moodle.org/security> until July 18th, to give you some time to fix your sites before these issues are made more public.

The easiest way to fix these issues on your site is to upgrade your Moodle sites to the latest stable release for the branch you are using (1.9.2, 1.8.6, 1.7.5, or 1.6.7) or latest weekly version. As usual you can get these from <http://download.moodle.org> or more conveniently via your local CVS mirror.

If you are confident patching your code, then most of the issues also have patches provided below.

MSA-08-0009: Persistent Cross-site Scripting (XSS) via blog entry title

Topic: Persistent Cross-site Scripting (XSS) via blog entry title

Severity: Major

Versions affected: <1.6.7, <1.7.5

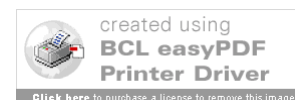
Reported by: ProCheckUp Ltd

Issue no.: MDL-15392

Solution: upgrade to 1.6.7, 1.7.5 or any recent nightly or use patch

<http://cvs.moodle.org/moodle/blog/lib.php?r1=1.38.6.3&r2=1.38.6.2>

Description:



ProCheckup discovered that 1.6.x and 1.7.x sites with enabled blogs are vulnerable to persistent Cross-site Scripting (XSS) attacks through blog entry titles. (Moodle 1.8 and later is not affected). We would like to thank them for informing us in a responsible manner and coordinating the disclosure of security advisories.

Credits: Adrian Pastor and Amir Azam of ProCheckUp Ltd. (www.procheckup.com)

MSA-08-0010: sql injection in HotPot module

Topic: sql injection in hotpot module

Severity: Major

Versions affected: <1.6.7, <1.7.5, <1.8.6, <1.9.2

Reported by: internal

Issue no.: MDL-15184

Solution: upgrade to 1.6.7, 1.7.5, 1.8.6, 1.9.2 or any recent nightly or use patch <http://cvs.moodle.org/moodle/mod/hotpot/report.php?r1=1.8.6.1&r2=1.8.6.2>

Description:

We have discovered that Hotpot module code in report.php is vulnerable to sql injection attacks.

MSA-08-0011: Potential webroot disclosures warning

Topic: Potential webroot disclosures warning

Severity: Minor

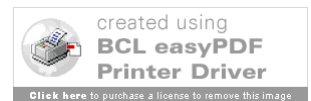
Versions affected: all versions

Reported by: ProCheckUp Ltd

Issue no.: MDL-15413

Solution: make sure display_errors is disabled in PHP configuration; 1.8.6 and 1.9.2 contains new warning for administrators

Description:



ProCheckup discovered that several scripts display errors if display_errors enabled in PHP configuration. This problem will be fully fixed in later Moodle versions because it requires modification of many files and review of all code from upstream, in the meantime the best fix is to make sure your server is configured properly - see <http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors>

Thanks to ProCheckup for informing us in a responsible manner and coordinating the disclosure of security advisories.

Credits: Richard Brain of ProCheckUp Ltd. (www.procheckup.com)

MSA-08-0012: Potential non-persistent XSS when searching for group members (MSSQL and Oracle only)

Topic: Potential non-persistent XSS when searching for group members (MSSQL and ORACLE only)

Severity: Minor

Versions affected: <1.9.2

Reported by: internal

Issue no.: MDL-15079

Solution: upgrade to 1.9.2 or any recent nightly or use patch

<http://cvs.moodle.org/moodle/group/members.php?r1=1.3.2.4&r2=1.3.2.5>

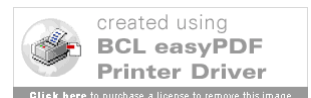
Description:

We have discovered that systems running on MSSQL or Oracle databases are vulnerable to non-persistent cross-site scripting (XSS) attack. This vulnerability was caused by incorrect escaping when using database engines which use Sybase style quoting (MSSQL and Oracle only).

MSA-08-0013: CSRF (Cross-site Request Forgery) on Moodle edit profile page

Topic: CSRF (Cross-site Request Forgery) on Moodle edit profile page

Severity: Major



Versions affected: <1.6.7, <1.7.5

Reported by: ProCheckUp Ltd

Issue no.: MDL-15450

Solution: upgrade to 1.6.7, 1.7.5 or any recent nightly or use patch

<http://cvs.moodle.org/moodle/user/edit.php?r1=1.112.2.4.2.1&r2=1.112.2.4.2.2> +

<http://cvs.moodle.org/moodle/user/Attic/edit.html?r1=1.88.2.3&r2=1.88.2.3.2.1>

Description:

ProCheckup discovered that the user profile page in 1.6.x and 1.7.x sites are vulnerable to CSRF (Cross-site Request Forgery) attacks. Versions 1.8 and above are not vulnerable due to increased protection enforced by our standard forms library. We would like to thank ProCheckup Ltd and not disclosing this issue before the vulnerability was addressed.

Credits: Amir Azam and Adrian Pastor of ProCheckUp Ltd. (www.procheckup.com)

MSA-08-0014: potential sql injection in events handling code

Topic: potential sql injection in events handling code

Severity: Minor

Versions affected: 1.9.0 and 1.9.1 only

Reported by: internal

Issue no.: MDL-15552

Solution: upgrade to 1.9.2 or any recent nightly; upgrade needed only if custom code uses Events API

Description:

During internal review it was discovered that the new Events framework might be vulnerable to sql attacks. This code is not currently used within Moodle core, but sites 3rd party modifications could be vulnerable. If you have any code using Events API please read the details in <http://tracker.moodle.org/browse/MDL-9983> on how to update your code to comply with this change. Please note that the changes in 1.9.2 are not backwards compatible.

MSA-08-0015: profiles of deleted users were accessible

Topic: sql injection in hotpot module

Severity: Major

Versions affected: <1.6.7, <1.7.5, <1.8.6, <1.9.2

Reported by: Debbie McDonald and Mauno Korpelainen

Issue no.: MDL-15516

Solution: upgrade to 1.6.7, 1.7.5, 1.8.6, 1.9.2 or any recent nightly or use patch <http://cvs.moodle.org/moodle/user/view.php?r1=1.123.2.8&r2=1.123.2.9>

Description:

Profiles of deleted users were accessible which allowed spammers to abuse user profiles on some sites. Also please make sure that you have "Force users to login for profiles" is enabled in admin settings if your site allows registering of new users.

MSA-08-0016: Email could be changed in profile without confirmation

Topic: Email could be changed in profile without confirmation

Severity: Major

Versions affected: <1.9.2, < 1.8.6

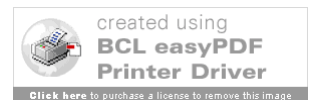
Issue no.: MDL-13811

Solution: upgrade to 1.9.2 or [1.8.6](#). Patch is provided at MDL-13811

Description:

In previous versions of Moodle, a user who is already authenticated could change their own email address without having to prove they could access the new email account, perhaps subjecting someone else to email from Moodle forums etc. In Moodle 1.8.6 and 1.9.2 a new setting called emailchangeconfirmation (default: on) now forces all users on the site to go through a confirmation process whenever they want to change their email account. Moodle 1.6.x and 1.7.x sites have not had this new feature added yet - we highly recommend upgrading to 1.9.x if this concerns you.


--



You are receiving this email because you registered a Moodle site with Moodle.org and chose to be added to this low-volume list of security notifications and other important Moodle-related announcements for Moodle administrators.

To unsubscribe you can re-register your site (as above) and make sure you turn the email option OFF in the registration form. You can also send a blank email to sympa@lists.moodle.org with "unsubscribe securityalerts" as the subject (from the email address that is subscribed).

See <http://lists.moodle.org/info/securityalerts> for more.

 **message-footer.txt**
1K
