osCommerce Online Merchant v2.3.2

osCommerce Online Merchant v2.3.2 is a security improvement release which improves the customer password forgotten routine and generation of random strings.

Previously, the customer password forgotten routine would automatically generate a random password and e-mail it to the customer. The code was based on tep_create_random_value(), the PHP mt_rand() function, and a weak seeding of the random number generator. Now, tep_create_random_value() uses Phpass' stronger get_random_bytes() method to generate random strings, and the customer password forgotten routine e-mails a personal link to the customer and gives them 24 hours to change their password. If they do not, they can continue to use their existing password and their personal password reset link is discarded.

The customer password forgotten routine is also now protected with a new Customer Password Reset Action Recorder module which, by default, limits the generation of personal password reset links to once every 5 minutes.

Changelog

- Changed customer password forgotten feature to e-mail a personal link to the customer where they can change their password up to 24 hours, instead of directly changing the password to a random string and e-mailing it to the customer.

  Added new password_reset.php page to manage personal password reset links.

  Added new ar_password_reset.php Action Recorder module to log and limit the request of personal password reset links to once every 5 minutes.

- Improve logic of tep_create_random_value() by using Phpass' random number generator.

  If function parameter $type is not 'mixed', 'chars', or 'digits', return a 'mixed' string instead of false.

- Add openssl_random_pseudo_bytes() and mcrypt_create_iv() to Phpass' get_random_bytes() class method. These are used if /dev/urandom is not available.

- Only seed the random number generator if PHP < 4.2 is used.

Upgrading from v2.3.1

The upgrade guide can be found online at:

http://forums.oscommerce.com/page/docs/_/oscom/23/release-notes-v2/oscommerce-online-merchant-v232-r12

The upgrade consists of:

- Adding two columns to the customers_info database table
- Modifying existing files
- Adding new files
- Updating language definitions
- Enabling the Customer Password Reset Action Recorder module

Files that have been modified in this release include:

admin/includes/classes/passwordhash.php
admin/includes/functions/general.php
includes/classes/passwordhash.php
includes/filenames.php
includes/functions/general.php
includes/languages/english/password_forgotten.php
includes/version.php
login.php
password_forgotten.php

Files that have been added to this release include:

includes/languages/english/modules/action_recorder/ar_reset_password.php
includes/languages/english/password_reset.php
includes/modules/action_recorder/ar_reset_password.php
password_reset.php

API Changes

tep_create_random_value() now returns a mixed string if the $type parameter is not mixed, chars, or digits. Previously a boolean false value was returned.

Language Definitions

The following language definitions have been modified:

modules/action_recorder/ar_reset_password.php

MODULE_ACTION_RECORDER_RESET_PASSWORD_TITLE
MODULE_ACTION_RECORDER_RESET_PASSWORD_DESCRIPTION

password_forgotten.php

TEXT_MAIN
TEXT_PASSWORD_RESET_INITIATED
EMAIL_PASSWORD_REMINDER_SUBJECT
EMAIL_PASSWORD_REMINDER_BODY
EMAIL_PASSWORD_RESET_SUBJECT
EMAIL_PASSWORD_RESET_BODY
SUCCESS_PASSWORD_SENT
ERROR_ACTION_RECORDER

password_reset.php

NAVBAR_TITLE_1
NAVBAR_TITLE_2
HEADING_TITLE
TEXT_MAIN
TEXT_NO_RESET_LINK_FOUND
TEXT_NO_EMAIL_ADDRESS_FOUND
SUCCESS_PASSWORD_RESET

Reference

A full list of source code changes can be seen at:

https://github.com/osCommerce/oscommerce2/compare/v2.3.1...upgrade232

Acknowledgements

We'd like to thank Gary Burton and George Zarkadas for testing and reviewing this upgrade guide, and George Argyros and Aggelos Kiayias for bringing the issue of insecure random number generators to our attention.