OX Guard
Release Notes for Release 2.6.0

November 30, 2016

Copyright notice

1 General Information

This release of OX Guard v2.6.0 for OX App Suite v7.8.3 has focused on becoming much more user-friendly, especially for basic users. Open-Xchange has recognized that some of the features and terminology was more orientated to advanced encryption users and thus was confusing for non-experts.

OX Guard now also provides:

- Full Encrypted File Support in OX Drive and OX Documents
- Simpler Guest Invitations

A more detailed overview of OX Guard v2.6.0 can be found at: `http://software.open-xchange.com/products/guard/doc/OX_Guard_Product_Guide_2_6_0.pdf`

Announcements

Open-Xchange encourages administrators to regularly update to the latest available release. In order to ensure a stable and up to date environment please note the different supported versions. An overview of the latest supported Major, Minor and Public Patch Releases can be found in the Knowledgebase at: `http://oxpedia.org/wiki/index.php?title=AppSuite:Version_Support_Committment`

2 Shipped Product and Version

Open-Xchange Guard 2.6.0-rev5

Find more information about product versions and releases at `http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering`

3 Vulnerabilities fixed with this Release

This section provides a summary of security related bug fixes that have been applied subsequently to shipping Release 2.4.2. Solutions for vulnerabilities have been provided for the existing codebase via Patch Releases.

45292 Padding oracle issue with guest authentication tokens
The access token for guest authentication was created based on AES256-CBC, which allows padding guessing. At the same time the OX Guard API responds differently in case the used padding was correct. As a result, attackers that obtained a encrypted authentication token and guest cookie could use brute-force mechanisms to decrypt the password in a short amount of time. Guard has been modified to respond with uniform error codes regardless if the guessed padding was correct or not, which makes the attack much harder. CVE-2016-4028

47878 XSS when decoding inline signatures
Malicious payload within signatures of Emails was executed in case the Email got decrypted using OX Guard. The component has been updated to use existing sanitization methods and drop usage of dangerous frontend-side functions. CVE-2016-6854, credits to Benjamin Daniel Mussler (@dejavuln).

47914 XSS/CSRF with public key content
Data from public PGP keys gets rendered at several places at the OX Guard frontend. When embedding script code, it can get executed since the related functions did not execute proper sanitization.

Several API endpoints of OX Guard were updated in order to sanitize user-generated public key content like comments or names. CVE-2016-6853, credits to secator.

48080 XSS at Guest templates
The external ”guest reader” website of OX Guard offers to provide a ID to select a visual template. This value was improperly handled and could be used to execute script code provided as parameter value. This got fixed by validating and limiting the provided value. CVE-2016-6851, credits to Benjamin Daniel Mussler (@dejavuln).

48509 XSS at Guest templates
A bypass was found for Bug #48080 that allowed attackers to work around the sanitizer. We’re now checking the provided values data type in a safer way. CVE-2016-7403, credits to Benjamin Daniel Mussler (@dejavuln)

48510 XSS at Guest Reader for mails
The external ”guest reader” website of OX Guard was not using the existing sanitizer, which allowed to execute script-code at Emails to guests. This got solved by properly sanitizing content provided at this interface. CVE-2016-7403, credits to Benjamin Daniel Mussler (@dejavuln)

48511 XSS for attachments at encrypted mails
When using attachments within encrypted mail, the content-type was incorrectly detected and certain sanitization mechanisms were bypassed. This got solved by performing independent analysis of attachments by OX Guard. CVE-2016-7403, credits to Benjamin Daniel Mussler (@dejavuln).

4 Bugs fixed with this Release

This section provides a summary of bug fixes and changes that have been applied subsequently to shipping Release 2.4.2. Some of the announced bug fixes may have already been fixed at the existing code-base via Patch Releases.

39798 Missing Guard options on re-login
In rare cases OX Guard options were unavailable once a user triggered a re-login. This has been caused by a race-condition when querying user permissions and capabilities and got solved by refactoring this logic in later releases.

41301 Wizard triggered while using third-party encryption
When using a browser-side encryption plugin like Mailvelope, the OX Guard wizard was started when selecting encrypted mail. Users may not want to use Guard if they decided to use Mailvelope, therefor we’re no longer starting this wizard if Mailvelope is used.

44077 Chrome asks to store users private-key password
When signing messages, certain browsers like Google Chrome recognized the private-key password field as a login area and ask to store the password. While storing passwords in a browser is convenient, the private-key password is used to validate a users identity and should not be available in a unencrypted storage.

44983 Timeout when decrypting huge files
In case a large file with several gigabytes gets decrypted, OX Guard sometimes ran into a hard-coded timeout. That timeout is now configurable as `com.openexchange.guard.connectionTimeout` if support for large files are a requirement and the environment needs higher timeouts.

44995 Missing upload bar for large files
When uploading large files for instant encryption, the upload bar was not shown in some conditions. This was solved.

45076 Bad error message for invalid recipients
When adding invalid recipient addresses and sending a mail via OX Guard, a quite cryptic error message was returned. This has been changed to a error message that helps to identify the invalid address.

45453 Missing branding an some spots
While the OX Guard product name is configurable to support branding and white-label services, the configured values were not used consistently when combining words. This has been fixes by using consistent combinations of branded and hard-coded strings.

45556 Errors when deleting users
Users get a pre-generated key assigned as long as they did not generate their own. When removing a user on a schema where no user has ever generated a own key, the associated deletion routine failed since the expected table was missing.

49906 Sending mail fails depending on size limits
In case a operator configured `MAX_UPLOAD_SIZE` with `0`, OX Guard was unable to send Email since that value got interpreted as "0 bytes" instead of "unlimited". The implementation has been changed to recognize `0` as unlimited at this place.

5 Changes relevant for Operators

5.1 Changes of Configuration Files

Change #3560 Configuration to determine if new Guests get a password email
New Guests can either receive a temporary password via email, or assign a password on first login. Therefor a new configuration option got added to the guard configuration file: `com.openexchange.guard.newGuestsRequirePassword` (Default: `false`).

Change #3534 Set a lifespan for the temporary tokens used for Guest reset
For guest users that don't have password recovery enabled, they can create new keys using a reset functionality. A confirmation email is sent containing a temporary token. The lifespan of the token is now configurable through `com.openexchange.guard.temporaryTokenLifespan` (Default: `48`).

Change #3647 New configuration options for controlling file buffering
Added two configuration options for controlling buffering behavior of Guard when processing file uploads. Guard does only buffer non sensitive or encrypted data to disk. This can now be configured using `com.openexchange.guard.fileUploadDirectory` (Default: `<empty>`) and `com.openexchange.guard.fileUploadBufferThreshhold` (Default: `10240`).

Change #3646 Option for forcing TLS for HKP via DNS SRV
Added an option for forcing TLS when connecting to HKP servers queried using DNS SRV lookup, `com.openexchange.guard.forceTLSForHKPSRV` (Default: `false`).

Change #3645 Sub-Configuration option to fail if no DNSSEC validated AD flag in SRV response
OX Guard queries the HKP server of a recipient's domain by performing a SRV DNS lookup. This change introduces a new option `com.openexchange.guard.dns.allowUnsignedSRVRecords` (Default: `true`) which discards SRV records which were not validated with an AD flag. We added a Sub-configuration option to fail if the DNSSEC validation for the requested SRV record fails, i.e. if the AD flag is not set, then assume there is no valid HKP server for this domain. If this option is not set, then the lack of validation is logged, but the lookup to the HKP server still takes place as normal. This enables the operator to check for potential failures in the logs before enabling "hard-fail".

5.2 Changes of Database Schema

Change #3533 New database table `temporary_tokens`
Due to adding a reset functionality to the Guest reader, we need an additional database table to store tokens on a temporary basis. This needs database storage as the timeframe may be days and different servers may be used. A database table `temporary_tokens` in the main OX Guard schema has been created that stores a random token, user the token was generated for, and the time created. This table can be used to verify a reset request. The related liquibase task is `2.4.3:create_temporary`

5.3 Changes of Behaviour

Change #3573 Content-Type detection of arbitrary data
The `com.j256.simplemagic` library got added to allow content-type guessing.

6 Tests

Not all defects that got resolved could be reproduced within the lab. Therefore, we advise guided and close monitoring of the reported defect when deploying to a staging or production environment. Defects which have not been fully verified, are marked as such.
To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server set-up for system and integration testing. All changes have been checked for potential side-effects and effect on behaviour. Unless explicitly stated within this document, we do not expect any side-effects.

7 Fixed Bugs

39798, 41301, 44077, 44983, 44995, 45076, 45453, 45556, 49906, 45292, 47878, 47914, 48080, 48509, 48510, 48511,