



Release Notes for Patch Release #2112

August 25, 2014

Security Patch Release

This Patch Release addresses critical vulnerabilities; please consider deploying it as soon as possible. Not deploying this Patch Release may result in remote service exploitation, security threats to users and exposure of sensitive data.

Detailed vulnerability descriptions will be publicly disclosed no earlier than five (5) working days after public availability of this Patch Release. There is no indication that one or more of these vulnerabilities are already getting exploited or that information about them is publicly circulating.

Copyright notice

©2014 by Open-Xchange AG. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of Open-Xchange AG. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

1 Shipped Product and Version

Open-Xchange AppSuite backend 7.6.0-rev16

Open-Xchange AppSuite frontend 7.6.0-rev11

Open-Xchange AppSuite usm 7.6.0-rev10

Open-Xchange AppSuite eas 7.6.0-rev8

Open-Xchange AppSuite office 7.6.0-rev9

Open-Xchange AppSuite documentconverter 7.6.0-rev10

Open-Xchange AppSuite documentconverter-api 7.6.0-rev9

Open-Xchange Readerengine 4.2.5-45

2 Bugs fixed since previous Public Release

This document provides a summary of bugfixes and changes that have been applied subsequently to shipping Patch Release #2097.

30599 Exporting calendar offers a .js file for download

When exporting a specific calendar folder, the exported CSV contains a corrupted format. It is not possible to track down this issue to a particular object, therefore corrupted recurring appointments get skipped and logging has been extended to track down the bad object.

33394 Message count is different in message list and selected pane when select all messages

This has been fixed by changing the calculation of selected messages.

33489 Password shows up in clear text while viewing personal error logs as user

If a user checked the "Error Logs" section of the UI, some requests may expose clear text passwords that the user has entered before. This information is not exposed to any external party, however to ensure privacy and remove unnecessary output, this has been fixed by replacing all (top-level) properties that contain the word "password" by "*****".

33620 CVE-2014-5235

CVSSv2: 5.7

33715 EAS fetches the mail twice instead of only one time

EAS clients fetched a mail twice because the mail source was not available on first fetch. This has been solved by completely providing the mail including source on the first request.

33834 CVE-2014-5236

CVSSv2: 7.4

33835 CVE-2014-5236

CVSSv2: 7.4

33836 CVE-2014-5237

CVSSv2: 4.4

33838 CVE-2014-5238

CVSSv2: 5.4

33839 CVE-2014-5234

CVSSv2: 5.7

33914 Cannot drop more than a user capability with a single RMI call

The batch statements to drop the +/- variants of user capabilities used a wrong parameter index. Therefore, just the first supplied capability got dropped when provisioning users via the RMI or SOAP interface. The parameter index when dropping the +/- variants of user capabilities has been corrected.

33918 I18n service for locale <locale> has no translation

The names of subscription sources have been passed to I18nService regardless if they were LocalizableStrings or not.

This has been fixed by introducing a new flag to selectively translate subscription sources names.

33919 CVE-2014-5238

CVSSv2: 5.4

33936 Displayname with ampersand not displayed correctly

Caused by incorrect usage of `..escape`.

This has been fixed.

3 Changes relevant for Administrators

3.1 Changes of Configuration Files

Change #2126 Added new config item `com.openexchange.documentconverter.blacklistFile` to `documentconverter.properties`

The list of external document content URLs that are not allowed to be loaded by the readerengine after loading a document.

The file itself contains a list of (newline separated) regular expressions. Each external URL is first checked against the list of blacklist URL regular expressions. If the external URL matches one blacklist entry, the external URL is then checked against the list of whitelist URL regular expressions.

The behavior in summary is as follows:

- If the URL is not blacklisted and not whitelisted, it is resolved at runtime.
- If the URL is blacklisted but not whitelisted, it is not resolved at runtime.
- If the URL is not blacklisted but whitelisted, it is resolved at runtime.
- If the URL is blacklisted and whitelisted, it is resolved at runtime.
- In boolean notation: `valid = (!blacklisted) OR whitelisted`

Please note that the regular expressions need to fully qualify the patterns that the URL should be checked against. Upper/Lower cases need to be handled by the regular expression as well. The file itself needs to be UTF-8 encoded to be read appropriately.

Default value: `"/opt/open-xchange/etc/readerengine.blacklist"`

Change #2127 Added new config item `com.openexchange.documentconverter.whitelistFile` to `documentconverter.properties`

The list of external document content URLs that are allowed to be loaded by the readerengine after an external URL matched a blacklist pattern.

The file itself contains a list of (newline separated) regular expressions. Each external URL is first

checked against the list of blacklist URL regular expressions. If the external URL matches one blacklist entry, the external URL is then checked against the list of whitelist URL regular expressions.

The behavior in summary is as follows:

- If the URL is not blacklisted and not whitelisted, it is resolved at runtime.
- If the URL is blacklisted but not whitelisted, it is not resolved at runtime.
- If the URL is not blacklisted but whitelisted, it is resolved at runtime.
- If the URL is blacklisted and whitelisted, it is resolved at runtime.
- In boolean notation: valid = (!blacklisted) OR whitelisted

Please note that the regular expressions need to fully qualify the patterns that the URL should be checked against.

Upper/Lower cases need to be handled by the regular expression as well. The file itself needs to be UTF-8 encoded to be read appropriately.

Default value: `"/opt/open-xchange/etc/readerengine.whitelist"`

Change #2128 Added new config item `com.openexchange.documentconverter.urlLinkLimit` to `documentconverter.properties`

The external URL link limit specifies the maximum amount of valid external internet URLs (filtered by blacklist and whitelist before), that are tried to get resolved by the engine when loading a document.

When this limit is reached, no more external internet URLs are resolved for the current document.

Please note, that this limit is not directly related to the amount of visible linked objects within the document. The code itself often needs to resolve one URL more than once or even twice to finish loading of the objects' content.

In addition, the URL link limit not only affects the amount of URLs, resolved within the viewer but also the amount of resolved URLs when printing or downloading a document, so that the appearance of a viewed and of a printed/downloaded document is similar in general.

Set to -1 for no upper limit or to 0 to disable the resolving of internet URLs completely

Default value: 200

Change #2129 Added new config item `com.openexchange.documentconverter.urlLinkProxy` to `documentconverter.properties`

The external URL link proxy config entry specifies a proxy server, that is used by the readerengine to resolve external links, contained within a document. Such links are e.g. external `http://` graphic links, that are going to be resolved during the filtering process of a readerengine instance.

Set this entry to the address of the proxy server: `host:port`

Recognized protocols for object URLs to be resolved by the proxy are: `http://`, `https://` and `ftp://`

Leave empty, if no proxy server should be used by the readerengine.

Default value: n/a

4 Tests

The Open-Xchange QA team has successfully verified all bug fixes that could be reproduced within a lab environment.

To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server setup for system and integration testing.

All changes have been checked for potential side-effects and effect on behavior. Unless explicitly stated within this document, we do not expect any side-effects.

5 Fixed Bugs

30599, 33394, 33489, 33620, 33715, 33834, 33835, 33836, 33838, 33839, 33914, 33918, 33919, 33936,