



Release Notes for Patch Release #3147

March 14, 2016

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

©2016 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 7.6.3-rev8

Open-Xchange AppSuite frontend 7.6.3-rev7

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

2 Vulnerabilities fixed since previous Public Release

This section provides a summary of bugfixes and changes that have been applied subsequently to shipping Patch Release #3120. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

44409 CVE-2016-2840
CVSSv2 6.4

3 Bugs fixed since previous Public Release

This section provides a summary of bugfixes and changes that have been applied subsequently to shipping Patch Release #3120.

38021 Task's start and due dates are specified incorrectly in the email

The wrong server time zone was used when formatting dates for the participant notification mail. Now the correct time zone UTC is used to format dates.

43119 JSESSIONID cookie not set after clearing browser cache

In case a valid HTTP session identifier is specified in the requests URI but no "JSESSIONID" cookie exists yet, an appropriate "Set-Cookie" header for creating that missing "JSESSIONID" cookie was not set in response. In customer specific login implementations this could lead to issues routing a user to the correct middleware machine. We now ensure that the "Set-Cookie" header is set in response to create a "JSESSIONID" cookie when a valid HTTP session identifier is specified in request's URI. This handling is only used if no "JSESSIONID" cookie exists yet.

43312 Firefox-only: Auto-save email drafts value <empty>by default

Wrong default value for auto-save email drafts.
This has been fixed by changing default value from false to 'disabled'.

43929 Some display names like "A, B" end up in problems while replaying

The comma is a delimiter. Works if properly quoted. When editing a token-field, double quotes are introduced which will lead to two pairs. "A B" works because no comma. "A, B" works because quoted. ""A, B"" does not work (as expected) because the comma is not quoted, we get two pairs ""A and B"".

This has been fixed by removing all quotes from token-field labels.

44021 Members of distribution lists get lost if malformed with trailing whitespaces

Trailing whitespace were not removed.
This has been fixed by removing trailing whitespaces before adding to collection.

44076 Adding bigger distribution lists takes nearly endless (up to 8 min) and CPU usages increases

Redraw was triggered on every item in the distribution list.
This has been fixed by redrawing only once after distribution list is added.

44128 Sorting E-Mail returns no results

On certain IMAP backends sorting E-Mail by "From" or "Subject" led to empty result lists. This has been solved by falling back to in-application sort in case a IMAP backend is unable to return sorted results.

44264 Caldav usage from Mac OS X 10.11.3 cause lost of calendar shares

The calendar client of OS X 10.11.3 uses (and expects) malformed principal URIs for sharing calendars.

This has been solved by workaround malformed principal URIs for OS X calendar clients.

44315 After update to 7.6.3 Vacation Notice with ':from' Tag not editable

Sieve scripts that contained the 'from' tag were not taken into consideration from the backend when parsing.

This has been fixed by introducing the ':from' tag for the vacation type and a new 'from' attribute in the JSON payload.

4 Changes relevant for Administrators

4.1 Changes of Configuration Files

Change #3134 Introduced configuration property to specify whether a fall-back to in-app sort is supposed to be performed

Introduced configuration property "com.openexchange.imap.fallbackOnFailedSORT" to file 'imap.properties' to specify whether a fall-back to in-app sort is supposed to be performed in case IMAP "SORT" command gets quit with a "NO" response.

Default value is "false"; meaning to return an appropriate error to requesting client.

5 Tests

Not all defects that got resolved could be reproduced within the OX QA 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 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.

6 Fixed Bugs

38021, 43119, 43312, 43929, 44021, 44076, 44128, 44264, 44315,