



Release Notes for Patch Release #5439
2019-10-16

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 fifteen (15) 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

©2019 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of OX Software GmbH. 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 7.10.2-rev14
Open-Xchange AppSuite frontend 7.10.2-rev13
Open-Xchange Documentconverter-api 7.10.2-rev3
Open-Xchange Documentconverter 7.10.2-rev5
Open-Xchange AppSuite office-web 7.10.2-rev6

Find more information about product versions and releases at http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering and <http://documentation.open-xchange.com/>.

2 Vulnerabilities fixed since previous Public Release

This section provides a summary of bug fixes and changes that have been applied subsequently to shipping Patch Release #5420. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

66594 CVE-2019-16717

CVSS: 2.2

67097 CVE-2019-16717

CVSS: 3.1

66538 CVE-2019-16716

CVSS: 2.2

3 Bugs fixed since previous Public Release

This section provides a summary of bug fixes and changes that have been applied subsequently to shipping Patch Release #5420.

66088 Mail - Compose - Request read receipt flag checked by default

This has been solved by ensuring a valid address is passed to "Disposition-Notification-To" header and that only a valid E-Mail address is accepted for "disp_notification_to" in JSON field.

66241 Attach as PDF to e-mail after making changes does not use the changed PDF

Same request parameters lead to same responses from the MW #getDocument Ajax handler. In case the request parameters don't change after revisionless save, the response will be the unchanged one.

This has been fixed by providing 'revtag' parameter when creating the attachment.

66393 Reset password for guest account fails

This wasn't a bug, it was a wording problem.

This has been solved by changing wording for the avatar dropdown of "Change Password" for guests. Was confusing with Guard Guest emails. Changed to "Add login password" or "Change login password". Adjusted title and button of dialog.

66483 Chrome: appointment is opened only after third click

Windows sends a mousemove event when only a mousedown event should be triggered resulting in the monthview to enter drag mode.

This has been fixed by introducing a deadzone of 5px before dragging is enabled.

66919 vCard import: BDAY ignored without YEAR

Unable to handle vCard v4 partian dates.

Now handling PartialDate for Birthday and Anniversary to solve this issue.

66928 UI crashes when opening mail

Some jQuery functions got stuck and prevented further code execution. This has been fixed by using native functions.

66933 Caldav doesn't sync all appointments

For CalDAV collections with many contained resources where the initial synchronization result gets truncated before a specific point in time, consecutive DAV:sync-collection requests with this intermediate token would get answered with HTTP 403 Forbidden due to the token being assumed out of range.

This has been fixed by encoding additional flags into generated sync-tokens to properly resume intermediate truncated responses.

67006 Renaming folder with initial asterisk results in lost folder

Was caused by wrong detection whether a move or a rename needs to be performed. Fixed check whether a move or a rename needs to be performed to solve this issue.

66865 AS-7.8.4 and DC-7.10.2: No page preview icons in Presenter and Popout View

It is now possible to use the documentconverter version 7.10.2 with older appsuite-backends.

67012 Invitation for all day appointments will be changed after Outlook user accepted the appointment and user accept changes

This was caused by a different used iTIP method. This has been fixed by adjusting used iTIP method.

67017 Sieve filter settings page lags/stops for a time when moving elements

Change listener called too frequent. Solution: debounce execution waiting for 30ms without further call.

67021 Saving draft emails merged

Address string was interpreted as a group name in case host is NIL when parsing an ENVELOPE address string.

This has been fixed by aligning behavior of Open-Xchange Middleware according to common IMAP server one. Assume "missing-domain" as host part of an E-Mail address in case host is NIL when parsing an ENVELOPE address string.

67027 User cannot edit some of his own appointments after update to 7.10.2

Inconsistent data for organizer/principal in the legacy storage was converted to a representation of the organizer that assumed an external entity.

This has been solved by ignoring principal if equal to organizer when reading from legacy storage, correct sent-by in organizer for already migrated events. Please mind that the update task to correct the wrong data in the storage is disabled by default in the hotfix, but can be enabled manually by setting the property "com.openexchange.calendar.enableCalendarEventCorrectOrganizerSent-ByTask" to "true" if needed.

67042 No print option in preview of eml

This has been solved by enabling print preview for embedded mail.

67047 Converting of ACE email-addresses with uppercase-chars not working

Accept upper-case ASCII characters as well for ACE->IDN conversion to solve this issue.

67067 Message not getting displayed correctly

There is a check to test if a file actually holds data based on some heuristics. That check leads to false-positive for the inline image attachments of the affected E-Mail.

Fixed check for possibly empty file data.

4 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 behavior. Unless explicitly stated within this document, we do not expect any side-effects.

5 Fixed Bugs

66088, 66241, 66393, 66483, 66919, 66928, 66933, 67006, 66865, 67012, 67017, 67021, 67027, 67042, 67047, 67067, 66594, 67097, 66538,