



Release Notes for Patch Release #3731

November 21, 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 OX Software GmbH. 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 7.8.2-rev16
Open-Xchange AppSuite frontend 7.8.2-rev16
Open-Xchange EAS 7.8.2-rev7
Open-Xchange Office 7.8.2-rev6

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 bug fixes and changes that have been applied subsequently to shipping Patch Release #3630. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

49014 CVE-2016-9309

CVSS: 5.3

49439 CVE-2016-9308

CVSS: 4.1

49847 CVE-2016-9309

CVSS: 3.7

49848 CVE-2016-9308

CVSS: 5.7

49912 CVE-2016-9309

CVSS: 4.3

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 #3630.

48344 User is not able to sent email to users on the same cluster after account is added as external

Now user are able to send emails after the user added an internal email address as external email.

48520 Printing with edge not working

Print preview was empty and printing does not print the email content.
Now the preview is displayed and it is possible to print with edge.

49086 About 1600 Mails can not be deleted at once, Script Timeout in Browser

Removing the mails one by one takes very long.
With this fix all mails are handled together and it is quite faster.

49141 Mail content only displayed on reply/forward

Mail content were not visible in all mails, actual mail content nested inside `<head>` element, which is removed for embedded display of foreign HTML content
Transfer non-head child elements to body to make the content visible.

49231 Filter rules: From condition "is exactly" doesn't work on email addresses

To filter for email addresses in a more comfortable way "Sender address" were included as condition type.

49236 Huge amount of Mail folder could not be found on mail server messages for non-existing folders

The message for "Mail folder could not be found on mail server" were known, actually by design, but not expected to happen that often.

The fix just excludes the inbox from the obfuscation, to reduce the amount of error messages.

49259 Attachment corrupted when open in browser

Generic detection for possible XML content leads to accidental XML escaping.

This has been fixed by excluding application content from XML escaping.

49374 Bad organizer mail address when invitating through the calendar

Under certain circumstances, the organizer value was built from the user's display name when serializing to iCal.

This has been fixed by using the user's e-mail address as organizer value if "primaryMail" is configured.

49689 Cloud symbol missing for DriveMails in certain views

This has been solved by adding missing extension for drivemail icon indicator.

49693 OX error- Message could not be found in the folder

Adjusted logging to not flood log files and have a more adequate log level for common cases in which an image cannot be retrieved.

49864 Full-day appointment will be displayed as a regular 24h appointment on Android

Specific clients rely on a certain order of the EAS protocol elements. <AllDayEvent> shall be sent after <StartTime>, <EndTime>. Microsoft Exchange Server for example does this.

Sending <AllDayEvent> after <StartTime>, <EndTime>.

49869 Upsell not triggered in onboard wizard for updater

No handling for caps with digits.

Adjusts regex and adds error message when trying to use commas in params.

49903 Recipient missing in to: on reply-to action the second time

If the lastname of the user is set to a single whitespace, the displayname was set to a single whitespace too. Tokens are trimmed and therefore, this token was not shown but still attached to the mail.

This has been fixed by trimming participant display name before checking emptiness and add email address to tokenfield if displayname is empty.

49909 Filename encoding wrong in drive mail

File name contains possible mail-safe encoding rendering shared item unreadable to user.

Safety check for possible mail-safe encoding and appropriate decoding solved this issue.

49920 Quote get single lined when using drive mail

Wrong text formatting on explicit plain text transport.

Solution: Proper text formatting in case user wants to send a plain-text message.

49964 Drive mails using main account name instead of alias

Display name is always determined by associated user.

Now choosing proper full name by given mail address.

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

5 Fixed Bugs

48344, 48520, 49086, 49141, 49231, 49236, 49259, 49374, 49689, 49693, 49864, 49869, 49903, 49909, 49920, 49964, 49014, 49439, 49847, 49848, 49912,