



Release Notes for Patch Release #3272

May 10, 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 7.8.1-rev11

Open-Xchange AppSuite frontend 7.8.1-rev10

Open-Xchange Office 7.8.1-rev8

Open-Xchange Documentconverter 7.8.1-rev8

Open-Xchange Documentconverter-API 7.8.1-rev8

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 #3239. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

45295 CVE-2016-4026
CVSSv3: 3.7

45312 CVE-2016-4026
CVSSv3: 3.7

45328 CVE-2016-4027
CVSSv3: 2.4

45363 CVE-2016-4045
CVSS: 3.7

45364 CVE-2016-4048
CVSS: 4.3

45366 CVE-2016-4046
CVSS: 7.2

45386 CVE-2016-4047
CVSS: 4.1

45401 CVE-2016-4045
CVSS: 3.1

45402 CVE-2016-4046
CVSS: 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 #3239.

44705 Usercopy - OX drive lists shared files

The order of db entries of folder children are changed if an openjdk java is used. This is probably caused by different Hashset implementations.

This has been fixed by using sorted sets for folder children during usercopy.

44708 Emails with multiple threads / forwards are printed nearly unreadable

Just missing CSS for blockquotes, browser defaults need too much space.

This has been solved by adding border, less padding on left side, no padding on right side.

44836 Deleteuser fails after a usercopy

No possibility to not reassign with deleteuser clt.

This has been solved by extending deleteuser clt with reassign and no-reassign parameter.

44877 Not possible to access mails in folder with \ in name

In case an emailfolder have a backslash in the foldername like "new\folder", emails were not loaded.

This has been solved by only removing backslashes before dots in emailfolders.

44923 Mail: moving a folder to "My Folders" always uses default0/INBOX

Moving a folder to the virtual "My folders" folder didn't consider altnamespace and moved to IN-BOX.

Solution: Considering altnamespace now. If set, move folder to "default0" instead.

45101 pdf2svg using boundless memory - Pushing system out of memory

No mechanism to limit the amount of virtual memory, that an externally started PDF tool process is allowed to use.

This has been fixed by adding a new config item 'com.openexchange.documentconverter.pdftoolMaxVMemMB' to the 'documentconverter.properties' configuration file. The implementation uses this value to limit the amount of memory for the PDF tool process.

45132 New lines added when editing Drafts

Replacing HTML-Tags does not discard outer HTML content.

This has been fixed by unwrapping remaining div and prevent auto-prepend newline when editing drafts.

45287 Mail without content can not be forwarded, UI hangs forever

It was not possible to forward emails with attachments only.

Simplified mail reference handling for attachment to solve this issue.

45296 Appointments will not be displayed in month view when timezone "-4:00 CDT Cuba" is set

Daylight Saving Time switch on Sundays if Sunday is the start of the week combined leads to weeks being painted twice (adding 6d 23h because of DST switch technically is still the same week).

This has been fixed by normalizing time to UTC before doing the math.

45356 After updating to 7.8.1 customer is getting a a generic "500 Internal Server Error" instead of a proper json error

A side effect of the changes performed for an other Bug caused that OXExceptions are outputted as HTML error pages.

This has been solved by restoring previous behavior when outputting OXExceptions.

45362 Signature: in case the imported picture is too big, error message not easy to understand

The error message in case the imported signature picture is too big was only containing the amount of bytes.

This has been fixed by enhancing the exception message (both display and log) to include a human readable format.

45391 Unable to remove password for drive shares via link

Server request did not contain the removed password.

This has been solved by sending password=null to remove it properly.

45507 Illegal format: An IO error occurred is displayed with no additional informations
Adjusted logging and error messages.

45529 OXUserCopyService doesn't copy aliases

User aliases were copied to user_attributes table instead of user_alias table.

Solution: Copy aliases to user_alias instead of user_attributes during usercopy.

4 Changes relevant for Administrators

4.1 Changes of Configuration Files

Change #3252 New config item com.openexchange.documentconverter.pdftoolMaxVMemMB for documentconverter.properties

A new config item 'com.openexchange.documentconverter.pdftoolMaxVMemMB' has been added to the 'documentconverter.properties' configuration file to allow the customer to limit the maximum amount of virtual memory, that an externally started PDF tool process is allowed to consume. If the given limit is reached, the process will immediately terminate and throw an exception in general, that is accordingly handled by the DocumentConverter implementation. If the item is set to -1, there will be no memory limit for the process. Any other positive value is treated as amount of Megabytes. The value should not be set below values of 50 (MegaBytes) to avoid immediate termination of a conversion process. The default value is set to 1024. Config entry:

```
# The maximum size in MegaBytes of virtual memory that
# a PDFTool instance can allocate;
# set -1 for no upper limit of maximum virtual memory
# Default value: 1024
com.openexchange.documentconverter.pdftoolMaxVMemMB=1024
```

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

44705, 44708, 44836, 44877, 44923, 45101, 45132, 45287, 45296, 45356, 45362, 45391, 45507, 45529, 45295,45312,45328,45363,45364,45366,45386,45401,45402,