



Release Notes for Patch Release #4256

2017-07-10

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

©2017 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 7.8.3-rev29
Open-Xchange AppSuite frontend 7.8.3-rev25
Open-Xchange EAS 7.8.3-rev9
Open-Xchange Office 7.8.3-rev10
Open-Xchange Office-Web 7.8.3-rev9

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 #4223. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

54403 CVE-2017-9809

CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)

54402 CVE-2017-9808

CVSS: 3.3 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)

54321 CVE-2017-9808

CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

54320 CVE-2017-9808

CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

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 #4223.

54532 Error message "Folder "INBOX" has been closed on mail server" confusing for end user

Confusing displayed error message.

Solution: Rephrased error messages dealing about connectivity issues to mail server to have a more user-friendly information. Moreover added the "Please try again later." suffix to hint to a possibly temporary nature of the issue.

54377 Generation of missing MD5 sums on filestore Objects causes high read load

There might be situations where the metadata for stored infostore documents does not indicate the referenced file's md5 checksum. This may be the case for files that were stored more than 4 years ago, or for files that have been uploaded in chunks, e.g. during a migration. When synchronizing via OX Drive, the missing checksums for those files are calculated on demand, which requires the files to be retrieved from the underlying storage. When having many or very large files where the checksum needs to be calculated for, this may lead to an increased read load which may impact other processes and systems in the installation.

This has been fixed by providing functionality to calculate missing file checksums on demand.

54349 Edge crashes on large attachments

Too much memory and cpu usage by canvas resize.

Integrate canvas resize into our lazyload mechanism so not every picture is processed simultaneously to solve this issue.

54348 Attachment filename wrong when forward email

Building the forwarded mail calling setHeader erased the header information about file name. This has been solved by calling setHeader first and set the file name header afterwards.

54311 Unable to send mail with onboard external account as sender

ALO SMTP server responds with multi-line greeting on socket connect which messed-up parsing of server's capabilities.

This has been solved by dealing with multi-line greetings from SMTP server.

54262 No timeout message if loading modules fails

No error message on require timeout.

This has been fixed by adding timeout message and reload option with longer timeout (30 seconds).

54177 Creating folders or renaming folders to prefix A- or B- does not show

The folder title gets not rerendered after a title change.

Now after a title change also the folder title gets rerendered.

53454 A folder called user is visible

Leftover namespace folder remains in LIST/LSUB collection.

This has been fixed by adding a special check that cares about dropping leftover namespace folders.

4 Changes relevant for Operators

4.1 Changes of Command Line Tools

Change #4236 New commandline tool calculatefilechecksums

There might be situations where the metadata for stored infostore documents does not indicate the referenced file's md5 checksum. This may be the case for files that were stored more than 4 years ago, or for files that have been uploaded in chunks, e.g. during a migration.

When synchronizing via OX Drive, the missing checksums for those files are calculated on demand, which requires the files to be retrieved from the underlying storage. When having many or very large files where the checksum needs to be calculated for, this may lead to an increased read load which may impact other processes and systems in the installation.

Therefore, a new commandline tool named 'calculatefilechecksums' is introduced, which allows to calculate such missing checksums on demand (operating either on a per context or database schema level).

5 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.

6 Fixed Bugs

54532, 54377, 54349, 54348, 54311, 54262, 54177, 53454, 54403, 54402, 54321, 54320,