Release Notes for Patch Release #3951

February 20, 2017

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

1 Shipped Product and Version

Open-Xchange AppSuite backend 7.8.2-rev25
Open-Xchange AppSuite frontend 7.8.2-rev22
Open-Xchange Office 7.8.2-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 bug fixes and changes that have been applied subsequently to shipping Patch Release #3917. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

50715 CVE-2016-10078
CVSS: 5.3

50716 CVE-2016-10077
CVSS: 4.3

50849 CVE-2017-5213
CVSS: 3.1

51038 CVE-2017-5863
CVSS: 4.3

51039 CVE-2017-5864
CVSS: 3.3

51058 CVE-2016-10078
CVSSv3: 3.6

51069 CVE-2017-5863
CVSS: 4.3

51164 CVE-2017-5210
CVSS: 3.6

51202 CVE-2017-5864
CVSS: 5.4

51219 CVE-2017-5864
CVSS: 5.4

51464 CVE-2017-5864
CVSS: 3.5

51474 CVE-2017-5864
CVSS: 4.3

51480 CVE-2017-5864
CVSS: 5.4

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 #3917.

8361 Login not possible if folder limit is reached
This has been fixed by adding missing handling for this special case. Now the login is working and the user gets notified about this error.

50039 Problem with folder rename of external storage providers
Dropbox identifies the folder through the path. New Files create all folders in their path by default. This is a special Dropbox behavior.
This has been solved by checking for folder existence before storing a file and return default "folder does not exist exception".

50414 Birthdays in the portal widget/sidepopup are sometimes a day off
Birthday calculation was slightly different in both views and apart from that even not correct for all cases.
This has been solved by using the same code for both views and also using a correct approach.

50689 Possible to lock files in external storages when not supported
The 'locks' capability was not correct for some external storages.
Changed behaviour: The file lock feature is disabled for every external storage. Lock does only work in the internal ox fileStore now.

50693 Content pane folder name not refreshed when renamed on external storage
Error handling is now done inside the apps. If errors with external storages (or other folder errors) appear and that folder is currently selected, the app will change to the default folder and reload the parent folder.

51053 Appointment invitations get duplicated by adding attachments
Deactivated Notification pool combined with multiple uploads of attachments result in a single notification mail for each attachment.
Solution: Keep track of a batch of attachment uploads during the whole stack.

51091 Upload to external filestorage account folder does not abort if overquota and fails
Missing error handling for overquota in multiple file upload.
This has been solved by checking error FLS-0024 and stop queue if this error appears. Also check for rate limit error. If one of those errors appear, the upload queue stops and removes all files from the queue.

51368 Bursts of WARN Messages: filemanagement.internal.ManagedFileManagementImpl ..Temporary file could not be deleted about 800-1000/day
Delete attempt does not check whether file is non-existing.
This has been fixed by properly checking if attempt is made to delete a non-existing file changed logging appropriately.

4 Changes relevant for Operators

4.1 Changes of Configuration Files

Change #3934 Disallow list-style-image style element
Disallow list-style-image style element in file
`whitelist.properties: html.style.list-style-image="u, none"`

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

8361, 50039, 50414, 50689, 50693, 51053, 51091, 51368, 50715, 50716, 50849, 51038, 51039, 51058, 51069, 51164, 51202, 51219, 51464, 51474, 51480,