Release Notes for Patch Release #4394

2017-10-17

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 7.8.4-rev14
Open-Xchange AppSuite frontend 7.8.4-rev14
Open-Xchange AppSuite Office 7.8.4-rev5
Open-Xchange AppSuite Office-Web 7.8.4-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 #4377. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

55703 CVE-2017-15029
CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N)

55651 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55603 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55602 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55601 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55600 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55090 CVE-2017-13667
CVSS: 6.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:L)

55068 CVE-2017-13668
CVSS: 3.7 (CVSS:3.0/AV:N/AC:H/PR:L/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 #4377.

55694 Html signature - images within the signature did not get saved into dedicated signature storage
Sometimes it was not possible to upload pictures into the dedicated signature storage.
Fixed a racecondition to solve this issue.

55679 Create a new signature with image alone - Save button at the bottom should be disabled till the image is saved
Missing handling for pending images.
This has been fixed by introducing cascade.

55606 Undocumented: imap4flags extension is a requirement not only for ”mail categorization” but also for custom sieve filter rules
Support for ’imapflags’ was removed for the new v2 api in 7.8.4.
This has been fixed by re-adding the support for the ’imapflags’ capability.

55574 Wrong sort order when using flag as sort option
Wrong sort order returned for ”flagged” sort field (660).
This has been solved by returning proper sort order for ”flagged” sort field (660).

55487 Contacts don't add correctly when choosing distribution list
This was caused by a missing check for contacts without mail address.
Now those contacts are filtered.

55413 OX Calendar Print Preview Issue
This was solved by dropping support for browsers built-in printing and give users a hint to use App-Suites print instead.

55409 Contact sort orders are inconsistent between ”address book” and ”select address dialog”
It was just sorted by the first character.
This has been fixed by adding recursion when letters are equal.

55362 Translation missing on upload timeout error
Missing string in i18n.
Added missing string to i18n, this is only the new string, the string itself is still not translated, the translation will be available with the next public patch.

55360 Potential XSS-Bug while handling Mail From
Possible control and/or white-space characters returned to clients.
This has been fixed by dropping control and/or white-space characters from E-Mail addresses.

55301 mail.filter.json.v2 - Certain rules created with ”not” conditions, including ”not exists” (header) ExistsTestCommandParser, are shown in the UI as the positive condition
Certain rules created with -not- conditions, including -not exists- could not be parsed correctly.
This has been solved by adjusting the parsing and added backend support for this behaviour.

55288 pdf.js progressive rendering floods OX logs with ”Connection reset by peer” errors on Chrome
Superfluous error logging for common case when client/end-user abruptly aborts the HTTP connection.
This has been fixed by adjusting logging for common case when client/end-user abruptly aborts the HTTP connection.

55271 File name incorrect Japanese characters
Fullwidth digits were replaced in file names.
This has been solved by allowing fullwidth digits in file names.

55044 OXTender for Outlook destroys SMIME signature
Possible empty line after multipart preamble was not maintained.
Force a blank line before start boundary when writing out multipart content to solve this issue.

54802 Duplicate entry for key PRIMARY Error on Update 7.8.2 to 7.8.4
Names were written to user attributes table with possible leading and/or trailing whitespaces.
This has been fixed by checking for duplicate user attributes after any leading and trailing whitespaces were removed.

4 Changes relevant for Operators

4.1 Changes of Behaviour

Change #SCR-54 The getRequired return type was changed to from String to List<String>
The Command interface was adapted from String `"getRequired()"` to `List<String> "getRequired()"`. This was needed to support both the imapflags and the 'imap4flags' capability.

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

55694, 55679, 55606, 55574, 55487, 55413, 55409, 55362, 55360, 55301, 55288, 55271, 55044, 54802, 55703, 55651, 55603, 55602, 55601, 55600, 55090, 55068,