



## **Release Notes for Patch Release #3148**

March 14, 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 Open-Xchange AG. 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 7.8.0-rev26

Open-Xchange AppSuite frontend 7.8.0-rev19

Find more information about product versions and releases at [http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning\\_and\\_Numbering](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 #3121. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

**44409 CVE-2016-2840**  
CVSSv2 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 #3121.

**43312 Firefox-only: Auto-save email drafts value <empty> by default**

Wrong default value for auto-save email drafts.

This has been fixed by changing default value from false to 'disabled'.

**43843 The file .drive-meta with checksum "123456" was not found at company**

In case of background changes related to the metadata of a folder or a contained file, the server may supply the client with a wrong checksum in a DOWNLOAD action for the folder's .drive-meta file.

This has been fixed by re-checking .drive-meta integrity prior signaling in DOWNLOAD action.

**43929 Some display names like "A, B" end up in problems while replaying**

The comma is a delimiter. Works if properly quoted. When editing a token-field, double quotes are introduced which will lead to two pairs. "A B" works because no comma. "A, B" works because quoted. ""A, B"" does not work (as expected) because the comma is not quoted, we get two pairs ""A and B"".

This has been fixed by removing all quotes from token-field labels.

**44036 SQL problem: Unknown column guestCreatedBy in where clause**

com.openexchange.share.impl.cleanup.ContextCleanupTask tries to clean up contexts on schemas which aren't updated yet.

This has been solved by skipping contexts on schemas which aren't updated yet.

**44128 Sorting E-Mail returns no results**

On certain IMAP backends sorting E-Mail by "From" or "Subject" led to empty result lists. This has been solved by falling back to in-application sort in case a IMAP backend is unable to return sorted results.

**44264 Caldav usage from Mac OS X 10.11.3 cause lost of calendar shares**

The calendar client of OS X 10.11.3 uses (and expects) malformed principal URIs for sharing calendars.

This has been solved by workaround malformed principal URIs for OS X calendar clients.

## 4 Changes relevant for Administrators

### 4.1 Changes of Configuration Files

#### **Change #3134 Introduced configuration property to specify whether a fall-back to in-app sort is supposed to be performed**

Introduced configuration property "com.openexchange.imap.fallbackOnFailedSORT" to file 'imap.properties' to specify whether a fall-back to in-app sort is supposed to be performed in case IMAP "SORT" command gets quit with a "NO" response.

Default value is "false"; meaning to return an appropriate error to requesting client.

## 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

43312, 43843, 43929, 44036, 44128, 44264,