



Release Notes for Patch Release #3571

September 26, 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-rev22
Open-Xchange AppSuite frontend 7.8.1-rev21
Open-Xchange USM 7.8.1-rev9
Open-Xchange Documents frontend 7.8.1-rev10

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 #3521. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

48230 CVE-2016-7546

CVSS: 5.4

48231 CVE-2016-7546

CVSS: 4.3

48282 CVE-2016-7546

CVSS: 2.2

48559 CVE-2016-7546

CVSS: 4.3

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 #3521.

47184 Forwarding mail expands CC area

When forwarding a E-Mail which has CC recipients, the resulting compose dialog did expand the CC area. This was caused by a missing model-reset when performing actions based on the original mail and has been solved.

47417 Listing large folders results in IE11 issues

When listing folders with more than 10.000 E-Mails and scrolling through them, IE11 did report script warnings. Those warnings were triggered by long-running JS actions. We optimized the handling of pagination when dealing with lots of mails to avoid triggering those warnings. On very slow machines this might still happen though.

47587 Cancelled appointment in Outlook not updated

When cancelling a group appointment in Outlook as organizer, the appointment for participants was not removed in case those participants did have "PIM" access permissions. This was caused by a server-client state conflict and has been solved.

47785 Rate-limit triggered when handling huge distribution list

When working with large distribution lists, usually more than 500 members, OX App Suite UI triggered a lot of unnecessary requests to get member information. Depending on the workflow and amount of members this could exceed the default rate-limit and effectively lock-out a user for several minutes. We have optimized which and how many calls are triggered when editing distribution

lists to avoid this scenario.

48599 Forwarding multiple E-Mails led to error

When forwarding multiple E-Mails via OX App Suite UI, a error was triggered. This has been a side-effect of another bugfix and got resolved. It's now possible again to forward multiple E-Mails as attachment to a single mail.

4 Changes relevant for Operators

4.1 Changes of Behaviour

Change #0000 Compatibility with Google Chrome on macOS

Due to IME (input method editor) changes at Google Chrome we had to restrict compatibility of OX Documents on macOS to Google Chrome 53 or newer in order to avoid corrupted documents. In case a users tries to edit a file in OX Documents with an older version, the file is opened as "read-only" and a notification is shown.

5 Tests

Open-Xchange has successfully verified all bug fixes that could be reproduced within a lab environment.

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

47184, 47417, 47587, 47785, 48599, 48230, 48231, 48282, 48559,