



Release Notes for Patch Release #3520

August 29, 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 7.8.0-rev38
Open-Xchange AppSuite frontend 7.8.0-rev30
Open-Xchange Office Web 7.8.0-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 #3465. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

47601 CVE-2016-6842
CVSS: 4.3

47602 CVE-2016-6843
CVSS: 4.3

47770 CVE-2016-6844
CVSS: 4.3

47774 CVE-2016-6846
CVSS: 4.3

47781 CVE-2016-6845
CVSS: 5.4

47790 CVE-2016-6849
CVSS: 7.1

47822 CVE-2016-6848
CVSS: 6.4

47824 CVE-2016-6850
CVSS: 4.3

47891 CVE-2016-6852
CVSS: 5.0

47898 CVE-2016-6847
CVSS: 4.3

47916 CVE-2016-6849
CVSS: 7.1

48083 CVE-2016-6850
CVSS: 4.3

48061
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 #3465.

48047 Random OOM during parsing mail

This was caused by excessive creation of (sub-)strings while trying to re-parse a weird, but possible start tag segment.

This has been fixed by improving detection of possibly contained HTML start tag and changed re-parse routine to avoid sub-string creation where possible.

4 Changes relevant for Administrators

4.1 Changes of Configuration Files

Change #3408 New property for RSS feeds to define allowed schemes

Added a new property to allow the definition of supported schemes for RSS feeds.

Key: `com.openexchange.messaging.rss.feed.schemes`

Description:

Defines the URL schemes that are allowed while adding new RSS feeds. An empty value means all (by URL supported) schemes are allowed.

Default: `http, https, ftp`

Version: `7.8.3`

Reloadable: `false`

Configcascade_Aware: `false`

Related:

File: `rssmessaging.properties`

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 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

48047, 47601, 47602, 47770, 47774, 47781, 47790, 47822, 47824, 47891, 47898, 47916, 48083, 48061,