



Release Notes for Patch Release #5275
2019-06-11

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 fifteen (15) 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

©2019 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of OX Software GmbH. 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 7.8.4-rev59

Open-Xchange AppSuite frontend 7.8.4-rev53

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 #5246. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

65132 CVE-2018-9997

CVSS: 5.4

64992 CVE-2019-11521

CVSS: 5.3

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 #5246.

63699 Feedback Module: When Skyscraper Advertisement is Collapsed the Expand Icon is Obfuscated by the Feedback Icon

Feedback button was located in io-ox-core.

This has been fixed by moving Feedback button to io-ox-screens.

64815 [object] Object on session timeout

Callback function was expecting a string.

This has been solved by making it work with strings and error objects.

65349 Signature with an image without text will not display

Also signatures with whitespaces were filtered.

This has been solved by adjusting the filter for signatures.

65366 JVM creates huge amount of WARN+ERROR loglines and 100% CPU for several hours 100%

Growing inconsistencies in general cache causing a massive amount of log messages keeping CPUs constantly busy.

Improved general caching to use a single map instead of trying to manage two resources (map & queue) for implementing LRU behavior.

4 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 behavior. Unless explicitly stated within this document, we do not expect any side-effects.

5 Fixed Bugs

63699, 64815, 65349, 65366, 65132, 64992,