



Release Notes for Patch Release #5508
2019-12-10

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 App Suite backend 7.10.1-rev25
Open-Xchange App Suite frontend 7.10.1-rev24
Open-Xchange office 7.10.1-rev5
Open-Xchange documentconverter 7.10.1-rev5
Open-Xchange readerengine 7.10.1-rev4

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 #5483. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

67871 CVE-2019-18846

CVSS: 6.5

67874 CVE-2019-18846

CVSS: 5.0

67931 CVE-2019-18846

CVSS: 5.0

67980 CVE-2019-18846

CVSS: 5.0

68136 CVE-2019-9853

CVSS: 7.7

68252 CVE-2019-18846

CVSS: 5.0

68258 CVE-2019-18846

CVSS: 5.0

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 #5483.

67017 Sieve filter settings page lags/stops for a time when moving elements

Change listener called too frequent.

Debounce execution waiting for 30ms without further call to solve this.

67286 Need for extended debug logging to trace registration/unregistration of permanent push listeners

Avoid loading context data when checking user validity.

68181 Read emails are displayed in bold font independent of read/unread status on MacOS

On MacOS, the sender is always bold because it's easier to read with many rows and MacOS and

iOS users are well trained by this style anyhow. Bold doesn't imply "unseen". In this case, however, there was also a little CSS bug. The date stayed gray for unseen messages; that's fixed. In addition, we set the sender now to extra-bold and dark black (#000) in order to have another visual decoration beyond the blue dot.

68253 High CPU min. 3 Threads with >95% CPU in "WeakHashMap()"

DateFormatCache was not threadsafe.

This has been fixed by using a synchronized map.

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

67017, 67286, 68181, 68253, 67871, 67874, 67931, 67980, 68136, 68252, 68258,