



Release Notes for Patch Release #5637
2020-03-09

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

©2020 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 7.6.3-rev50

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 #5537. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

MWB-34 CVE-2020-8543

CVSS: 3.1

68441 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 #5537.

MWB-116 OOM, backend/hazelcast crashes frequently

Many unnecessary cache invalidation events related to "User" cache region due to recording the time stamp of last login.

This has been solved by only updating user attribute if it actually was changed, skip cluster-wide invalidation.

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

MWB-116, MWB-34, 68441,