



Release Notes for Patch Release #6090
2022-02-10

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

©2022 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 backend 7.10.6-rev9
Open-Xchange App Suite frontend 7.10.6-rev6
Open-Xchange App Suite imageconverter 7.10.6-rev3
Open-Xchange App Suite documentconverter-api 7.10.6-rev3
Open-Xchange App Suite documentconverter 7.10.6-rev4
Open-Xchange App Suite office-web 7.10.6-rev4
Open-Xchange App Suite hazelcast-enterprise 7.10.6-rev3

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 #6093. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

MWB-1366 RCE in log4j <2.15.0 (CVE-2021-44228)

Updated logback logging framework to newest version containing a fix.

MWB-1350 CVE-2022-23099

CVSS: 3.5

DOCS-4161 CVE-2022-24405

CVSS: 7.3

DOCS-4120 CVE-2022-24406

CVSS: 6.4

OXUIB-1172 CVE-2022-23101

CVSS: 4.3

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 #6093.

DOCS-4105 comments are ahead of 1 hour

Different behavior of OX Text and Word compared to the other apps. This difference was no longer adapted after introducing the comments with mentions for OX Text in 7.10.5.

MWB-1372 JVMs/Groupware-Nodes crashing with high CPU and RAM inside of the JVM, no login possible

Caused by heavy thread contention at "java.security.Provider.getService(String, String)"
Replace Java Security Providers with service-caching instances to avoid heavy thread contention at "java.security.Provider.getService(String, String)".

MWB-1408 7.10.5 runupdate Connection closed by the other side

Missing supplemental upgrade packages for Hazelcast Enterprise were added.

MWB-1409 OX EAS authentication remains rate-limited after temporary auth backend out-

age

Previous rate limit implementation could lead to "starving" of incoming login requests due to sliding window behavior.

Use 3rd party library "bucket4j" for more robust rate limit implementation, which does refill of tokens in intervally manner.

MWB-1414 Error in SQL syntax in the following statement on schema

Possible indefinite growth of database statements due to many accessible folders.

Perform partitioned infostore search for larger amount of folders now.

MWB-1444 new mails can not be composed after installing Patch 6084 when having many external accounts configured

Plain connection established although SSL connection expected.

Orderly signal whether a direct SSL connection should be established or not.

OXUIB-660 User can remove read permissions to (default) calendar results in inaccessible calendar

There was a missing check for admin rights.

Do not filter the calendar if the user has still admin rights.

OXUIB-1222 ui glitch in mail list view when marking mails with 'star'

There was simply a "float:right" missing.

4 Changes relevant for Operators

4.1 Changes of Packaging

Change #SCR-991 New packages to aid rolling cluster upgrades with Hazelcast Enterprise

In order to connect to a legacy Hazelcast cluster running a previous version of Hazelcast Enterprise with transport layer encryption, and broadcast invalidation events while database update tasks are executed, the following new packages are provided:

- open-xchange-cluster-enterprise-upgrade-from-7103-7104
(containing new bundle com.openexchange.hazelcast.enterprise.upgrade312)
- open-xchange-cluster-enterprise-upgrade-from-7105
(containing new bundle com.openexchange.hazelcast.enterprise.upgrade411)

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 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.

6 Fixed Bugs

DOCS-4105, MWB-1372, MWB-1408, MWB-1409, MWB-1414, MWB-1444, OXUIB-660, OXUIB-1222, MWB-1366, MWB-1350, DOCS-4161, DOCS-4120, OXUIB-1172,