Release Notes for Patch Release #6089

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

1 Shipped Product and Version

Open-Xchange App Suite backend backend 7.10.5-rev38
Open-Xchange App Suite frontend 7.10.5-rev30
Open-Xchange App Suite imageconverter 7.10.5-rev10
Open-Xchange App Suite documentconverter-api 7.10.5-rev6
Open-Xchange App Suite documentconverter 7.10.5-rev6
Open-Xchange App Suite office-web 7.10.5-rev9
Open-Xchange App Suite hazelcast-enterprise 7.10.5-rev5

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 #6092. 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 #6092.

MWB-1408 Runupdate Connection closed by the other side
Missing supplemental upgrade packages for Hazelcast Enterprise were added.

DOCS-3981 Lots of "DC caught an exception" ERROR messages in groupware.log
Mail server related exceptions might occur when accessing attachments via provided MW API but should be filtered out for logging for a dedicated set of exceptions.
Logging should occur on DEBUG/TRACE level for a defined set of mail server exceptions (to be evaluated). Severe errors/exceptions need to be still logged as errors. According to information from backend team, responsible for provided mail API and thown exceptions when accessing Mail API, OXException categories USER_INPUT and PERMISSION_DENIED should only be logged on DEBUG level. All other OXExceptions are logged according to the categories log level, set at exception itself.

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-1444 New mails can not be composed after installing latest Patch 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.

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.

DOCS-4104 Errors after updating imageconverter, duplicate entry PRIMARY
Some kind of call sequences might lead to insertion of duplicate DB rows with primary keys in update case, although a previous delete call already happened. This seems to be caused by DB server concurrency issues with some deployments.
Due to the use of MySQL using an 'INSERT INTO ... ON DUPLICATE KEY UPDATE ...' statement instead of just using the SQL standard 'INSERT INTO...' call prevents concurrency issues with updated rows on DB server side by using the UPDATE part of the call if row still exists after a call to DELETE.

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-1409 OX EAS authentication remains rate-limited after temporary auth backend outage
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.

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

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

MWB-1408, DOCS-3981, DOCS-4105, MWB-1444, MWB-1414, DOCS-4104, MWB-1372, MWB-1409, OXUIB-660, OXUIB-1222, MWB-1366, MWB-1350, DOCS-4161, DOCS-4120, OXUIB-1172,