# OX®

# **Release Notes for Patch Release** #5972

2021-03-15

<span style="color:red">**Security Patch Release**</span>

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 7.10.4-rev20
Open-Xchange App Suite frontend 7.10.4-rev21
Open-Xchange App Suite usm 7.10.4-rev4
Open-Xchange App Suite documentconverter-api 7.10.4-5
Open-Xchange App Suite documentconverter 7.10.4-rev5
Open-Xchange App Suite office 7.10.4-rev8
Open-Xchange App Suite documents-collaboration 7.10.4-rev8
Open-Xchange App Suite office-web 7.10.4-rev8

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 #5960. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

**DOCS-3201   CVE-2021-28095**
CVSS:3.1

**DOCS-3200   CVE-2021-28094**
CVSS:3.1

**DOCS-3199   CVE-2021-28093**
CVSS:3.1

# 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 #5960.

**MWB-799   Optimize FolderMapManagement cache**
Inefficient max. size restriction of in-memory folder cache.
This has been fixed by using the SessionD events when the short term sessions are removed and use the Guava cache's expireAfterAccess method with a decent max time that should only remove stale entries.

**MWB-855   Memory Leak: DefaultDispatcher caches are never cleaned**
The caches implemented by ConcurrentMaps are never cleaned and can leak for e.g. requests that include rest-like endpoints like mail attachment downloads.
This has been fixed by using Google cache with expiration of 30 minutes on non-accessed instead of a regular map, which holds entries forever once put into it. Moreover, several caches storing information grabbed from DispatcherNotes are folded into one cache.

**MWB-854   Memory Leak: DatabaseFolderStorage.STAMPS is never cleaned**
Collection of context-associated time stamps might grow constantly.
This has been fixed by clearing collection of context-associated time stamps when last session for a certain context terminates.

**MWB-888   Increased load since 7.10.3**
Too many occurrences of low-level HTTP end-point pools for initialized Sproxyd clients.

This has been fixed by adding cache for low-level Sproxyd HTTP end-point pools.

**MWB-954   Wrong HTTP status code when If-None-Match header is set**
No response status distinction for read-only operations in If-None-Match/If-Match checks.
This has been solved by using HTTP 304 response during If-Match/If-None-Match checks for GET and HEAD.

**OXUIB-514   Attachments deleted from draft return after saving draft**
Draft was saved before all delete requests were processed.
This has been solved by waiting for all delete requests to be resolved, also if draft gets deleted.

**DOCS-3239   Presentation Template - Scroll issues**
When an image is inserted via the buttons in template drawings, the mousedown happens on the content root node, but the mouseup does not.  But these events are registered for an optional scrolling.  Therefore the scroll position was not correctly adapted, when the user changes the slide using the slide pane and does not click at least once into the document after inserting the image. This has been solved by checking the target nodes for mousedown and mouseup events that are required for scrolling.

**DOCS-3222   Default templates have wrong review language in places**
Templates contained more than 5 different languages on XML level.
This has been fixed on XML level, replaced all (western) lang attrs to be only en-US for EN templates, de-DE for DE templates.

**DOCS-3248   Automatic color in shape shows black, then reverts to white after save**
The filter cannot evaluate type 'auto' for text colors in shapes (Presentation and Spreadsheet, ooxml). Solution: Instead of sending 'auto' when the user selects 'Auto' as a text color, the best text color is evaluated corresponding to the shape background.  This calculated color is sent to the filter.

**OXUIB-726   Distribution list entries wrong after editing the list**
A combination of changes and streamlining caused loss of firstname and lastname, company was used as fallback.
This has been solved by adding available data were possible so company name is not used as fall-back, prefer display name over company name for external participants.

**USM-17   Status code 403 (FORBIDDEN): No such session**
Lifetime of USM sessions to the OX backend are much shorter now for the OX backend as expected by USM.
This has been fixed by setting parameter staySignedIn=true at http-api call for login.

**DOCS-3237   Cell content does not get saved when using 'save as' if cell is still "open"**
Document was not flushed before the copy was created in Drive.  Flushing causes to save all pending changes which, in Spreadsheet, includes to commit the cell edit mode.
Solution: Flush document before starting to copy the file in Drive for user actions "Save As" and "Save As Template".

**MWB-967   Higher load on parsing sent email**
Was caused by possible long-running Matcher.find() invocation.
This has been fixed by adding fast plausibility check & introduced a timeout-aware matcher alternative that respects a passed timeout whenever matching the input sequence or finding a certain sub-sequence is requested to avoid possibly long-running matcher invocations.

**MWB-958   Not possible to change directly case of context name with changecontext**
Context names are checked case-insensitive for equality when attempting to change a context's name and thus changing to the same context name, but different cases was considered as a no-op. This has been solved by checking case-sensitive for equal context names when attempting to change a context's name.

**MWB-951   Share is not created if mailbox is overquota**
Missing special handling for error codes that advertise actual transport succeeded, but append to standard sent folder failed.
This has been fixed by adding special handling for error codes that advertise actual transport succeeded, but append to standard sent folder failed.

**MWB-892   Different words in OX for the same - Beschreibung, Notiz., Anmerkung**
Inconsistent translation of 'notes'.
This has been fixed by adjusting translations.

**MWB-966   'Object not found. USE_COUNT' 'error comparing objects' errors in Logs**
Missing mapping for "use count" field.
This has been solved by adding missing mapping for "use count" field.

# 4   Changes relevant for Operators

## 4.1   Changes of Configuration Files

**Change #SCR-818   New parameter to control login behavior of USM client**
After the semantics of the login action were adjusted with SCR-418 (store action dropped, staySignedIn flag added), sessions created by the USM service on the middleware may time out too early in default configurations.  Therefore, a new property is introduced through which the USM client will pass the staySignedIn parameter during the login action, defaulting to true.
To control the behavior, the new property com.openexchange.usm.ox.stay_signed_in is added in configuration file usm.properties as follows:
```
# Specifies for Connections whether to stay signed in (avoids expiration of running sessions
to the OX server).
# Default: true
com.openexchange.usm.ox.stay_signed_in=true
```

**Change #SCR-834   Configuration to change CalDAV display name for standard folders**
com.openexchange.caldav.standardFolderDisplayName
CalDAV display name for the standard folder. Placeholder [foldername] and [owner] are possible. [foldername] is the localized String of default folders.
Default is [foldername].
Parameter is reloadable but not config cascade aware (always server wide).

**Change #SCR-835   Configuration to change CalDAV display name for shared folders**
com.openexchange.caldav.sharedFolderDisplayName
CalDAV display name for shared folders. Placeholder [foldername] and [owner] are possible. [foldername] is the localized String of default folders, or the folder name as-is for non-default folders.
Default is [foldername] ([owner]).
Parameter is reloadable but not config cascade aware (always server wide).

# 5   Changes relevant for Developers

## 5.1   Changes of internal APIs

**Change #SCR-819   Introduced an extended update task service**
Introduced an extended update task service to properly log and throw exceptions when running update tasks for contexts and schemata.

# 6 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.

# 7 Fixed Bugs

MWB-799, MWB-855, MWB-854, MWB-888, MWB-954, OXUIB-514, DOCS-3239, DOCS-3222, DOCS-3248, OXUIB-726, USM-17, DOCS-3237, MWB-967, MWB-958, MWB-951, MWB-892, MWB-966, DOCS-3201, DOCS-3200, DOCS-3199,