Release Notes for Patch Release #5971

2021-03-15

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 7.10.3-rev34
Open-Xchange App Suite frontend 7.10.3-rev29
Open-Xchange App Suite office 7.10.3-rev14
Open-Xchange App Suite office-web 7.10.3-rev10
Open-Xchange App Suite documentconverter-api 7.10.3-rev4
Open-Xchange App Suite documentconverter 7.10.3-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 #5959. 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

DOCS-3201 CVE-2021-28095
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 #5959.

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.

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-903 One user can create stacktraces to JE >36.000 lines (and >5 MB size)
Equal exceptions chained multiple times.
This has been solved by avoiding chaining equal exceptions multiple times.

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-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-799 Optimize FolderMapManagement cache
Was caused by inefficient max. size restriction of in-memory folder cache.
This has been solved 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.

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.

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-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".

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.

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

OXUIB-514, MWB-951, MWB-903, MWB-888, MWB-855, MWB-854, MWB-799, DOCS-3248, DOCS-3239, DOCS-3237, DOCS-3222, DOCS-3201, DOCS-3200, DOCS-3199, DOCS-3201,