Release Notes for Patch Release #6189

2022-11-02

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 Version

Open-Xchange App Suite backend 7.10.6-rev30
Open-Xchange App Suite frontend 7.10.6-rev20
Open-Xchange App Suite office 7.10.6-rev6

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 #6178. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

DOCS-4580 CVE-2022-42889
CVSS: 9.8

MWB-1882 CVE-2022-42889
CVSS: 9.8

MWB-1784 CVE-2022-43697
CVSS: 4.3

OXUIB-1795 CVE-2022-37306
CVSS: 4.3

OXUIB-1933 CVE-2022-43696
CVSS: 4.3

MWB-1823 CVE-2022-43698
CVSS: 5.0

MWB-1862 CVE-2022-43699
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 #6178.

MWB-1830 USM/EAS: Internal server error
USM/EAS client is requesting too many emails with too much information, which is too dangerous for the middleware in terms of memory consumption and unfortunately must be prevented so that the middleware process remains responsive.
Don't put restrictions on such requests in case associated client is USM/EAS to solve this issue.

OXUIB-1885 Folder 'confirmed_spam' not listed in folder tree
This was caused by conflicting lists of (default-)folders: io.ox/mail//defaultFolders and list of types in folders/extensions.js
This has been solved by removing hardcoded entry in folders/extensions.js

OXUIB-1879 Calendar entry not in selected color as created
This was caused by missing check for organizer rights.

Now checking for organizer rights and render as disabled if applicable. Info: We decided that the organizer shall not affect the participant's calendars folder color. The appointment will always appear in the participant's folder color. In the edit mode, the color setting for non-organizers will be disabled.

OXUIB-1827 Mail not displayed - content is only visible via view source or as forwarded mail
Mail included an element with height of 100%.
This has been solved by setting height of root/html tag within iframe to 0 to lever out the 100% height - but only for mails with sender Paypal.

MWB-1395 OX middleware java thread issue
An individual thread is used to perform asynchronous session storage tasks. In case Hazelcast gets unresponsive, those threads pile up rendering the system unresponsive as too many threads need to be handled by JVM.
This has been solved by introducing separate worker(s) for issuing operations against Hazelcast-backed session storage.

OXUIB-1089 Drivemail: missing autoswitch when coming from drive 'send by email'
When using the "send by email" function from drive, the quota is not checked.
When using the "send by email" function from drive, the quota will now be checked accordingly and DriveMail will be used if necessary.

OXUIB-1714 Unexpected and inconsistent success message shown when updating external account
When a new account is created, it is classified as "new" until a refresh is executed. Therefore, "Account added successfully" is displayed until the refresh.
Solution: A newly created account is now only recognized as new when it is created. Afterwards, "Account updated" is used.

MWB-1811 Deletion of shared folders not possible if guest changed permissions of shares
Guest users who were invited with "author" permissions can adjust permissions of newly created folders, hence remove the sharing user later on.
This has been fixed by ensuring internal entity is admin, prevent permission changes by guests.

OXUIB-1917 Browser Not Supported Page Stays in the Cache because of permanent redirect
Before http code 301 was used that caused the browser to cache the redirection to unsupported.html (301 represents "Moved permanently").
Now http code 302 is used that should not cache the redirection at all (302 represents "Moved temporarily").

4 Changes relevant for Operators

4.1 Changes of Packaging

Change #SCR-1159 Upgraded Apache Commons Text
Upgraded Apache Commons Text from v1.9 to v1.10.0 in com.openexchange.bundles

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-1830, OXUIB-1885, OXUIB-1879, OXUIB-1827, MWB-1395, OXUIB-1089, OXUIB-1714, MWB-1811, OXUIB-1917, DOCS-4580, MWB-1882, MWB-1784, OXUIB-1795, OXUIB-1933, MWB-1823, MWB-1862,