Release Notes for Patch Release #5719

2020-05-12

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 7.10.2-rev26
Open-Xchange App Suite frontend 7.10.2-rev23
Open-Xchange USM 7.10.2-rev6
Open-Xchange EAS 7.10.2-rev7

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 #5676. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

MWB-226 CVE-2020-12644
CVSS:3.1

MWB-221 CVE-2020-12645
CVSS:3.1

MWB-190 CVE-2020-12646
CVSS:3.1

MWB-120 CVE-2020-12645
CVSS:3.1

MWB-108 CVE-2020-12643
CVSS:3.1

MWB-107 CVE-2020-12645
CVSS:3.1

MWB-70 CVE-2020-12646
CVSS:3.1

DOCS-1886 CVE-2020-12646
CVSS:3.1

DOCS-1844 CVE-2020-8542
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 #5676.

USM-1 EAS can't send mails when umlauts in loginname
The e-mail address of the user with umlauts in the domain name is directly used as from address for sending the e-mail. USM does replace the from address in the e-mail delivered by the client with the internally set e-mail address.
This has been fixed by converting the domain part of the users e-mail address to punny code when building the EAS-configuration.

USM-4 Continuous “429 Too Many Requests HTTP error code” messages
Because the root cause is not known this is just an improvement: Handle symptom after the rate limiter has blocked further login requests and try to avoid retries by the client. Currently USM returns HTTP status 200 (with error status content in the EAS protocol response). Now USM returns 429 with header ”Retry-After” with the same time period as returned by the backend.

OXUIB-218 Wrong link creation for MS Teams invitation after adding to calendar
Caused by UI urlify function (detect links in plain text). This function did some wrong encoding.
This has been fixed by removing useless encoding.

OXUIB-184 IE11 shows less columns in launcher pop-up
IE11 has sometimes issues with calculating dropdown dimensions.
This has been fixed by using fixed width in IE11.

OXUIB-166 Signatures in Plain text mails are with a blank line
Was casued by wrong Blocknode detection.
This has been solved by adjusting Blocknode detection.

OXUIB-148 App Launcher does not react on every second tap on smartphones
Backdrop added for dropdowns on mobile catches clicks and is not removed after dropdown closed.
This has been solved by making sure backdrop element gets removed if dropdowns close.

OXUIB-131 Distribution list saves with invalid entry
Error message did not prevent saving, success message from saving overwrote the error message.
This has been solved by stopping saving if there is an error so the user has a chance to notice the error message.

OXUIB-129 Composition spaces gets duplicated for some reasons
Remove handlers all work on same list of points regardless of the fact one of those handlers already removed a point, was caused by a race condition.
This has been improved by maintaining a list of deleted ids and further removeRestorePoint calls remove those points again if needed.

MWB-202 Brute-force-logins from one IP leads to denial-of-service (reject with 500 for all logins) after some minutes
Accumulation of HTTP sessions through massive number of incoming HTTP requests steadily spawning a new HTTP session. For example, if the server used only cookie-based sessions, and the client had disabled the use of cookies, then a session would be new on each request.
This has been solved by avoiding accumulation of HTTP sessions through massive number of incoming requests. Invalidate unused/unjoined as well as non-authenticated HTTP session. Moreover, ensure removal of invalid session cookies.

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

USM-1, USM-4, OXUIB-218, OXUIB-184, OXUIB-166, OXUIB-148, OXUIB-131, OXUIB-129, MWB-202, MWB-226, MWB-221, MWB-190, MWB-120, MWB-108, MWB-107, MWB-70, DOCS-1886, DOCS-1844,