Release Notes for Patch Release #4472

2017-12-12

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 five (5) 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 AppSuite backend 7.8.3-rev41
Open-Xchange AppSuite frontend 7.8.3-rev35
Open-Xchange AppSuite office7.8.3-rev12
Open-Xchange AppSuite office-web 7.8.3-rev11

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 #4440. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

56352 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

56157 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

56091 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

56063 CVE-2017-17061
3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

56056 CVE-2017-17062
3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N)

56055 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55882 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55830 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55167 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

54915 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

51464 CVE-2017-17060
5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

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 #4440.

52523 NPE at com.openexchange.subscribe.mslive.MSLiveApiClient.getAccessToken
Added the missing service to the activator to solve this issue.

54957 This message has been truncated due to size limitations. Show entire message - no images can be loaded
Accept new 'forceImages' parameter for 'mail?action=get&view=document' action. Also show extended action label only when external images are filtered out.

55831 Upon external drive account deletion, the UI still triggers requests that lead to errors
This has been fixed by adding a missing folder refresh.

55964 High load on ConfigDB since update to latest Patch
Excessive "SELECT cid FROM context_server2db_pool WHERE server_id=xxx AND write_db_pool_id=xxx AND db_schema=xxx´ ´ queries.
This has been solved by optimizing collecting data for drive metric calculation and improved some locations which invoked 'getContextsInSameSchema()'.

56034 OAuth not working if ending on other nodes
JVM route information was not added to redirecting call-back URL.
Now ensure JVM route is added to redirecting call-back URL.

56071 Mail content not displayed
Garbled mail messes up IMAP server's BODYSTRUCTURE information.
This has been solved by reparsing mail manually in case IMAP server's BODYSTRUCTURE information is messed up.

56140 Cloud-Storage connection problem
Wrong check if whether used connection pool is currently unused/empty caused premature stopping of idle-connection-closer.
Proper check whether used connection pool is currently unused/empty to solve this issue.

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 behaviour. Unless explicitly stated within this document, we do not expect any side-effects.

5 Fixed Bugs

52523, 54957, 55831, 55964, 56034, 56071, 56140, 56352, 56157, 56091, 56063, 56056, 56055, 55882, 55830, 55167, 54915, 51464,