Release Notes for Patch Release #4473

2017-12-13

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 7.8.4-rev19
Open-Xchange AppSuite frontend 7.8.4-rev17
Open-Xchange AppSuite office 7.8.4-rev6
Open-Xchange AppSuite office-web 7.8.4-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 #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.

56149 Userreporting ERROR ”Cannot find user with identifier <id> in context <ctx> ”
When storing the report before sending it, a useless comma was added.
This has been solved by constructing correct JSON when loading macdetails from local storage.

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.

56107 OX - Slowness in loading the mail folder list
List request breaks on altnamespace with many folders.
This has been fixed by removing ’default0’ list request out of ’virtual/standard’.

56089 Not possible to delete account via API
Wrong owner identifier passed to quota-aware file storage instance.
This has been fixed by compiling proper owner info when resolving a file storage.

56073 Logging the IMAP endpoint IP
Remote IP address of connected end-point was not available.
Now also output remote IP address of connected end-point to solve this.

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.

56038 Name of attachment with Japanese characters not correctly displayed
”ISO-8859-1” charset is assumed for every string value in MAPI properties of a TNEF-encoded attachment.
This has been solved by detecting proper charset (e.g. by code page attribute) and use that to get the string value.

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.

56023 External Storage error while saving presentations created from a template
Generating setDocumentAttribute operation twice. In renameHandler and during reloading the document.
Marking document as unmodified before reloading it to solve this issue.

56021 Feedback: comments and suggestions area without checks filters and escaping
Some characters haven’t been sanitized.
More sanitizing for feedback exports solve this.

55974 Appointments in public calendars are getting displayed in the same color independent of the status
Changed default status from accepted to unconfirmed due to some issues with itip attachments.
This has been fixed by using status accepted as default for public appointments.

55972 Mail not displayed correctly in App Suite UI
Garbled HTML content with conditional revealed comments confuses Jericho HTML parser.
Get rid off HTML comments prior to processing to display such mails.

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()'.

55948 Mailadresses not in "Collected addresses" when reading a new Mail
"collect_addresses" field extracted out of wrong JSON object.
This has been solved by extracting "collect_addresses" field out of proper JSON object.

55865 Source Maps Support in Appsuite Development
Modification of source code from middleware before evaluation.
This has been solved by stop modifying source code on the client side.

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.

55102 Cloud storage - moving of a larger folder / larger number of files between different storages stops after 1100s with error 502
Possible HTTP proxy timeout during long-running operations.
Introduced the possibility to let a client submit a certain operation to a job queue, which can be frequently polled to check operation's status.

55085 Tasks: error message on removing editor
Removing oneself as a participant caused permission loss. Which was treated as an error.
Don't treat permission loss as an error anymore as this is expected in this case now.

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.

52633 Drag & drop of a huge picture into a HTML-Mail will cause the JVM to OOM up until OS swapped
Missing failure handling of tinymce. Remove the image manually.
This has been solved by removing image preview if upload of image fails due to whatever reason (for example, when the image size is too big).

4 Changes relevant for Operators

4.1 Changes of Configuration Files

Change #4505 Introduce new UI setting
Introduce ui mail setting 'transform/multipleEmptyLines' (default: true). This settings simply allows to disable the described default behavior.

4.2 Changes of Packaging

Change #SCR-61 Added new bundle c.o.ajax.requesthandler.jobqueue.json
Added new bundle com.openexchange.ajax.requesthandler.jobqueue.json to open-xchange-core package.

5 Changes relevant for Developers

5.1 Changes of the HTTP API

Change #SCR-60 Added new job queue JSON interface
Introduced the possibility to let a client submit a certain operation to a job queue, which can be frequently polled to check operation's status.

Change #SCR-76 Accept new 'forceImages' parameter for 'mail?action=get&view=document' action
In case 'view=document' is specified for for 'mail?action=get' action the new URL parameter 'forceImages' is accepted to control whether HTML images are allowed in mail's HTML content.

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

7 Fixed Bugs

56149, 56140, 56107, 56089, 56073, 56071, 56038, 56034, 56023, 56021, 55974, 55972, 55964, 55948, 55865, 55831, 55102, 55085, 54957, 52633, 56352, 56157, 56091, 56063, 56056, 56055, 55882, 55830, 55167, 54915, 51464,