Release Notes for Patch Release #5340

2019-07-29

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 AppSuite backend 7.10.1-rev17
Open-Xchange AppSuite frontend 7.10.1-rev16

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 #5309. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

66094 CVE-2019-14225
CVSS: 6.4

66081 CVE-2019-14227
CVSS: 5.4

66025 CVE-2019-14227
CVSS: 5.4

65805 CVE-2019-14226
CVSS: 3.1

65799 CVE-2019-14226
CVSS: 3.1

65722 CVE-2019-14226
CVSS: 2.2

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 #5309.

66184 Quite a lot long running threads hanging in mail compose via sproxyd
Uploaded files are directly streamed to destination storage with the consequence that reading from stream blocks possible file storage resources (e.g. connection in connection pool) for the time the actual upload is in progress. That behavior leads to more and more threads stacking up awaiting connections from connection pool. That huge amount of threads lets ”VM Thread” run permanently leading to constant ”stop the world” pauses making machine unresponsive.
Solution: Spool uploaded files to temporary file to not block storage resources (e.g. connection pool) by possibly slow upload. Introduced a timeout (default is 30 seconds) when waiting for an available connection in HTTP connection pool. Changed filestore connectors to be responsive to ConnectionPoolTimeoutException.

66162 Basic user can not create a new calendar by uploading an ics
This was caused by wrong root folder.
This has been solved by always using the default (personal calendar) folder as root folder.

65970 Contact Print Action ‘details’ option is displaying City, State and Postal code in Dif-

ferent lines
This has been solved by introducing locale/format to allow country specific address formatting.

65943 Umlauts not correctly synced via CalDAV with iOS devices
A problem in the serialization logic for extended properties of calendar components caused non-ASCII characters being corrupted during saving.
Properly encode extended properties of calendar components during saving to solve this issue.

65941 Removing ro from db safely
A superfluous check led to the "unregisterdatabase" utility reporting that also read-only schemas are possibly "in use".
This has been solved by performing "in use" check during "unregisterdatabase" for master database only.

65581 Refused to display in a frame because it set 'X-Frame-Options' to 'sameorigin'
Regular expression in link parser was too greedy which led the parser to not append the appropriate attributes target and rel attributes to the link.
This has been solved by fixing the regular expression.

65552 Invalid recipient in Drivemail leads to inconsistent behavior
In case multiple transport mails are supposed to be sent, the whole operation fails in case send attempt for one mail fails.
Solution: Do not abort sending multiple transport mails if send attempt for one mail fails.

65515 Failed to load email message content in UI
Corrupted mail with invalid multipart delimiters and invalid charset name quoting leads to failure when parsing/displaying the affected mail.
Solution: Deal with possibly quoted charset names on charset look-up. This fixes the exception when looking-up charset by charset name, but does not display reasonable content since multipart delimiters are corrupt in mail's source. The user sees: This mail has no content.

4 Changes relevant for Operators

4.1 Changes of Behavior

Change #SCR-496 Country specific post address formatting moved into separate component
Country specific postal address formatting was handled as part of translations before. Now formatting is part of the regular App Suite frontend logic ('io.ox/core/locale/postal-address.js') using the country part of user's current locale.

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

66184, 66162, 65970, 65943, 65941, 65581, 65552, 65515, 66094, 66081, 66025, 65805, 65799, 65722,