Release Notes for Patch Release #2333

January 12, 2015

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.

1 Shipped Product and Version

Open-Xchange AppSuite backend 7.6.1-rev14

Open-Xchange AppSuite frontend 7.6.1-rev11

Open-Xchange AppSuite documentconverter 7.6.1-rev7

2 Bugs fixed since previous Public Release

This document provides a summary of bugfixes and changes that have been applied subsequently to shipping Patch Release #2336.

33399   Incorrect Polish translation in 7.6.0
Missing translations were added.

35168   Adding a hash sign to a SIEVE rule breaks the mail backend
This has been fixed by checking '#' as literals and not as comments when inside of double quotes.

35502   OX6 uploads a files greater than MAX_UPLOAD_SIZE before throwing the error "Request rejected because its size (573.93 MB) exceeds the maximum configured size of 10.0 MB"
Possible upload quota restriction were not considered during upload, but only checked afterwards. This has been fixed by applying max. file size and max. overall size when processing upload to abort uploading data once a threshold is exceeded.

35525   When no contact in folder, exporting folder should prompt users then quit exporting contacts not exporting empty file
There was no verification if a folder holds data.
This has been fixed by implementing a verification.

35641   'Duplicate transport account for user x in context yz' at RdbMailAccountStorage.updateMailAccount
The check for a duplicate transport account fields false positives in case transport server credentials are supposed to be taken from the mail settings.
Solution: Do not perform check for duplicate transport account in case transport server credentials are supposed to be taken from the mail settings. The preceding duplicate check for mail account is sufficient then.

35693   High CPU-Load after update to 7.6.0-32
The HTML sanitizer gets called unnecessarily for binary content due to wrong conditional expression that checks for possible HTML content. Sucking that binary content as UTF-8 interpreted string into memory and in turn applying calculation-intensive sanitizing operation to that string troubles both - Java Garbage Collector and CPU.
Solution: Fixed conditional expression to check for possible HTML content.

35695   Linked contacts from different folders cannot be displayed
Programmatically selecting a folder acts a little bit different, old selections were not removed triggerChange in selection used first found marked folder (css selector on class 'selected') this caused opening the first folder in the list (top down order) that where marked as selected.

35727   Widgets are showing different colors depending of load-order of css rules
Missing css namespace for all social widgets has been added.

35737   Document converter with loadbalancer
The problem was related to inappropriate HttpSession creation/handling in the case of stateful begin/get/end conversion cycles.
This has been fixed by creating a new HttpSession only in order to do proper JESSIONID handling

for stateful begin/get/end call cycles.

35784   Class file.storage.CURRENT_VERSION returns String "null"
If NULL is returned as version information for a file's meta data "...&version=null" gets passed from App Suite UI to server.
This has been fixed by checking for that special "...&version=null" URL parameter and interpret it as NULL.

35806   Birthday portal widget counts days backwards for next-year birthdays
UI calculated the days until birthday by using a timestamp that is always set in the current year.
Solution: If the birthday would be in the past we use the correct next years birthday now.

35863   UI freezes when clicking directly on attachment name using an iPad
The UI just injected an overlay to allow fixed positioning for those drop-downs. No freeze, but the UI was unreachable below that overlay. Collided with Bootstrap's own click backdrop for touch devices.
This has been fixed by using different selector to avoid a collision with Bootstrap's backdrop solution, close on click.

35889   CVE-2014-9466
CVSSv2: 6.0

35891   OAuthfor Box.com and Dropbox should not be activated as Default
Some authentication implementations have been enabled per default.
Thias has been fixed by disabling various OAuth bundles by default through setting associated "com.openexchange.oauth.¡provider-name¿" properties to "false".

35948   Error while changing settings for outgoing server for an external email account like gmail
Missing check for a valid prepared SQL statement prior to attempting to execute it.
Solution: Check for a valid prepared SQL statement prior to attempting to execute it.

3   Changes relevant for Administrators

3.1   Changes of Packaging

Change #2231   Removed some remnants from packaging
Contained within the 7.6.1 release are the new non-production ready and not supported filestore packages. Unfortunately the release documentation fails to mention that these packages are not for production or covered by support. It is for this reason that we strongly advise all our customers to uninstall those specific packages from their production systems (open-xchange-file-storage-boxcom, open-xchange-file-storage-dropbox, open-xchange-file-storage-googledrive and open-xchange-file-storage-onedrive). Of course you will be able to install the stable version of these packages once they are released for production.

4   Tests

Not all issues that got resolved with this Patch Release could be reproduced within the OX QA lab. Therefore, we advise guided and close monitoring of the reported issue when deploying to a staging or production environment.
To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server setup 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

33399, 35168, 35502, 35525, 35641, 35693, 35695, 35727, 35737, 35784, 35806, 35863, 35889, 35891, 35948,