Release Notes for Patch Release #3521

August 29, 2016

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 7.8.1-rev20
Open-Xchange AppSuite frontend 7.8.1-rev19
Open-Xchange Office Web 7.8.1-rev9

Find more information about product versions and releases at `http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering`

2 Vulnerabilities fixed since previous Public Release

This section provides a summary of bugfixes and changes that have been applied subsequently to shipping Patch Release #3514. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

47601 CVE-2016-6842
CVSS: 4.3

47602 CVE-2016-6843
CVSS: 4.3

47770 CVE-2016-6844
CVSS: 4.3

47774 CVE-2016-6846
CVSS: 4.3

47781 CVE-2016-6845
CVSS: 5.4

47790 CVE-2016-6849
CVSS: 7.1

47822 CVE-2016-6848
CVSS: 6.4

47824 CVE-2016-6850
CVSS: 4.3

47891 CVE-2016-6852
CVSS: 5.0

47898 CVE-2016-6847
CVSS: 4.3

47916 CVE-2016-6849
CVSS: 7.1

48083 CVE-2016-6850
CVSS: 4.3

48061
4.3

3 Bugs fixed since previous Public Release

This section provides a summary of bugfixes and changes that have been applied subsequently to shipping Patch Release #3514.

46189 Unable to see Halo or who reserved a resource within the Scheduling tool
No single general solution for all different use cases in this scenario.
Solution: Introduced ui setting `'io.ox/calendar//freeBusyStrict'` (default: true), when NOT in strict mode detail view is available, details for appointments are not displayed.

46628 The facet "folder" is mandatory and has to be set
The error was a race condition in folder selection for search.
This has been fixed by only using visible/enabled options.

47184 Forwarding mails with cc-recipients automatically opens cc field in mail compose
On model creation data from the original mail was propagated that should have been omitted.
This has been fixed by omitting original mail data, now the cc filed is not open automatically.

47378 Contact csv import: error message very vague
The csv parser is configured to be tolerant and accepts rows in csv files with columns sizes lower than the number of title columns. If a row does not contain enough columns it will add empty columns at the end of the row. If a column in the middle of the row is missing all other entries will be shifted to the left. This leads to an error for the distribution list column, because the importer uses the data of another column for this field.
This has been fixed by adding a new parameter "line_number" to the response result entry in case of an error, because it's impossible to improve the handling of defective csv files.

47664 Empty object_permission table causes stale RDBMS connections
A database connection was not returned to the pool under specific circumstances.
This has been solved by ensuring database connection is returned to pool.

47683 Mail is not displayed correctly - 2 instead of three attachments
The regex pattern to identify the uuencoding wasn't able to handle umlauts.
This has been fixed by improving the regex pattern to recognize umlauts.

47932 No free mailstore found causes configdb inconsitencies
When deploying a new cluster, having not yet registered a mailstore, creating a context caused inconsitencies in the configdb.
This has been solved by running delete method of all registered plugins in case of a failure in postCreate of any of the registered plugins.

48006 IMAP ID is sent after login instead of before
"ID" command gets issued after login happened, breaking Dovecot's session tracing.
This has been fixed by moving signaling IMAP session identifier through "ID" command to pre-login state.

48047 Random OOM during parsing mail
This was caused by excessive creation of (sub-)strings while trying to re-parse a weird, but possible start tag segment.
This has been fixed by improving detection of possibly contained HTML start tag and changed re-parse routine to avoid sub-string creation where possible.

48118 Upsell I-Frame does not open in Firefox and IE
Click delegate on premium container didn't worked as expecting.
This has been solved by using default select handler and call upsell method via custom trigger.

4 Changes relevant for Administrators

4.1 Changes of Configuration Files

Change #3408 New property for RSS feeds to define allowed schemes
Added a new property to allow the definition of supported schemes for RSS feeds.

```
Key: com.openexchange.messaging.rss.feed.schemes
Description:
Defines the URL schemes that are allowed while adding new RSS feeds. An empty value means
all (by URL supported) schemes are allowed.
Default: http, https, ftp
Version: 7.8.3
Reloadable: false
Configcascade_Aware: false
Related:
File: rssmessaging.properties
```

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 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.

6 Fixed Bugs

46189, 46628, 47184, 47378, 47664, 47683, 47932, 48006, 48047, 48118, 47601, 47602, 47770, 47774, 47781, 47790, 47822, 47824, 47891, 47898, 47916, 48083, 48061,