Release Notes for Patch Release #4050

April 4, 2017

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-rev20
Open-Xchange AppSuite frontend 7.8.3-rev18
Open-Xchange Office 7.8.3-rev7

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 bug fixes and changes that have been applied subsequently to shipping Patch Release #4016. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

52255 CVE-2017-6912
CVSS: 4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

51863 CVE-2017-6913
CVSS: 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

51667 CVE-2016-10078
CVSS: 3.6 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:L)

51622 CVE-2017-6912
CVSS: 6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/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 #4016.

51839 Certain serious (non UCE/UBE) HTML mail is not displayed
Too greedy check for possibly malicious content led to this issue.
This has been solved by allowing properly parsed start tag.

52518 Compatibility fix for Debian and systemd
The Debian project did rename the initial process from `systemd` to `init` when moving to Debian 8.7. Some areas of our startup scripts depend on this name to determine whether systemd is used or not. We're now querying `/proc/1/comm` to figure out the kind and name of process that takes care about inits.

52437 oxsysreport tries to read nonexisting files
When running `oxsysreport` while having OX Guard installed, false-positives for password blacklisting could occur. As a result errors were reported by the `oxsysreport` tool, which has been solved by adjusting the regular expression for parameter blacklisting.

52314 Unicode decoding fails for multi-line mail subjects
In case a E-Mail subject spans multiple lines where each consists of UTF-8 mail-safe base64 encoded characters, decoding partly failed and Unicode characters were displayed in a scrambled way. This has been solved by properly handling such split subjects and encoding each part independently.

52238 Typo at NRFILES property at startscript
A typo at the `/opt/open-xchange/sbin/open-xchange` script led to a situation where custom config-

ured ”nofiles” limits where not correctly applied to the process. This has been solved by correcting the properties name and adding a log message to `open-xchange-console.log` in case the process fails to set this limit.

52235 Missing custom favicons
Newer versions of Firefox use the largest icon presented as `<link rel="icon">` as favicon, which defaults to a unbranded OX icon. Originally this handling was introduced to set a ”homescreen” icon when using the appropriate functionality on mobile operating systems. This was solved by removing the corresponding tag when using desktop operating systems.

52198 Applying OX Drive folder permissions recursively
A feature backport has been performed to allow recursive inheritance of OX Drive folder permissions when changing a parent folder.

52161 Missing mails on mobile devices when using mail categories
When using mail categories with a desktop browser and moving mails to specific categories, those mails would not be displayed at Inbox anymore when using the same account using a mobile browser. We solved this by avoiding categorization Inbox if the corresponding feature set is not available on the currently used platforms.

52151 Drop zone for .eml not disappearing if a file is not dropped with firefox on Windows
Firefox does not trigger dragleave or mouseout correctly.
This has been fixed by using mouseenter to remove the dropzone when the mouse enter the window without dragged files.

52157 IMAP master-auth user name provided to client
In case of specific IMAP errors related to `EXPUNGE` commands, a detailed error message was returned to the user, which could contain a user-name for IMAP master authentication. This was solved by removing detailed error message contents for that IMAP command.

52181 Firefox drop-zone overlaps mail list
When using a specific series of gestures while importing a .eml file to a mailbox, a Firefox bug on Windows and macOS got triggered which kept the ”drop zone” visible after dropping the file outside of the browser window. This subsequently blocked other user interaction with the mail list. We added a workaround for this browser bug in a way that clicking outside the drop zone will revert its state.

52123 Unable to change mail account name with certain mail configurations
If a user was changing its mail account displayname while the middleware uses a ”global” `mailServerSource` setting, incorrect host names were applied. As a result the displayname could not be changed. We solved this by applying the appropriate host name to avoid erroneous responses during the operation.

52104 Untraceable database timeouts during share cleanup
Once the `PeriodicCleaner` task for shares was executed, potential SQL errors could not be traced since the related schema name was unknown. To allow further debugging we added `com.openexchange.database.schema` as parameter for this cleanup run. It will highlight which database schema triggered timeouts or other errors.

51997 Shares created via Drivemail requested credentials
When sending a mail attachment and using ”Drive Mail” a password was requested even though a user did not enable this option. This could happen in cases where a user first specified a password but then un-ticked the related option. We solved this by checking the options state more carefully prior to creating the related share.

51967 Missing distribution lists in Outlook
When syncing Outlook using USM, certain amounts and combinations of contacts and distribution lists could lead to a situation where only a subset of contacts but not all distribution lists got synced.

This has been solved by sorting the type of object (contact, distribution list) prior to performing the sync operation. This way the kind of objects retrieved at the client side stays consistent in case the total amount of objects exceeds the chunk size for one sync operation.

51918 Calendar conflicts with UTC+12 timezones
During conflict detection, the floating time-span of full-day appointments was calculated using the servers timezone (usually UTC) while other appointments used the timezone configured by the user. In cases where a large offset to UTC is present, there has been a 50/50 chance that appointments would conflict with full-day appointments at the previous or next day. We're now calculating both values using the users specific timezone for conflict handling. This should bring down the probability of incorrect conflicts considerably.

51462 Full-day appointments could not be converted with Lightning
When using Thunderbird/Lightning and CalDAV of OX App Suite, full-day appointments could not be converted back to normal appointments using the CalDAV client. The reason for this was a client-specific CalDAV header used to indicate full-day appointments which caused issues with Lightning. We removed this header if the associated user-agent does not expect it.

51399 Repeated mail sending when using Outlook
In case a backend error did occur, like downtime of the mail storage, there could be situations where Outlook clients using USM get into a sending-loop, resulting to duplicated E-Mail. Those kind of errors are now handled by the USM API in accordance to the OX App Suite middleware error code.

51222 Long loading times for documents with certain storages
In case a large document gets requested off a slow cloud storage, very long loading times could happen and expected timeouts were not considered. This has been solved by adding additional timeouts that will kick in if a API request to the storage layer takes longer than anticipated.

51074 Encoding issues with passwords
In case certain operating systems got configured incorrectly, specifically RHEL6 and SLES11, usage of the `open-xchange-passwordchange-script` plugin could lead to incorrectly encoded passwords passed over to a script. This has been solved by adding an optional parameter as described by Change #4022 to allow base64 encoded transfer. Additionally, unexpected encoding configurations will get logged to `open-xchange-console.log` to alert operators about potential follow-up issues.

50918 Timezone issues with task start/due dates on negative timezone offsets
When defining a start or due date for tasks while using a negative UTC offset, the selected date would be reported incorrectly. This has been solved by adjusting the full-day handling for tasks to the calendar implementation which uses UTC.

49236 Messages regarding missing E-Mail
Some OX App Suite UI requests did lead to error messages regarding E-Mail which could not be found. After analyzing the situation, we suspect that there is a issue with obfuscated folder names. A fallback has been added in case decoding a folder name failed.

4 Changes relevant for Operators

4.1 Changes of Configuration Files

Change #3972 New property 'com.openexchange.folderstorage.inheritParentPermissions' (lean configuration)
Introduced new property `'com.openexchange.folderstorage.inheritParentPermissions'`. Set to true, to apply parent folder's permissions when moving a folder into the public folder tree.

Change #4022 Add option to base64 encode parameters handed to passwordchange script
Add new lean configuration parameter:

```
com.openexchange.passwordchange.script.base64
description:  Indicates if the string based script parameters like username, oldpassword
and newpassword should be encoded as Base64 to circumvent character encoding issues on improperly
configured distributions not providing an unicode environment for the process.
defaultValue:  false
reloadable:  true
configcascadeAware:  false
related:  com.openexchange.passwordchange.script.shellscript
file:  change_pwd_script.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 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.

6 Fixed Bugs

51839, 52518, 52437, 52314, 52238, 52235, 52198, 52161, 52151, 52157, 52181, 52123, 52104, 51997, 51967, 51918, 51462, 51399, 51222, 51074, 50918, 49236, 52255, 51863, 51667, 51622,