Release Notes for Patch Release #5509

2019-12-11

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 App Suite backend 7.10.2-rev19
Open-Xchange App Suite frontend 7.10.2-rev17
Open-Xchange eas 7.10.2-rev3
Open-Xchange office 7.10.2-rev4
Open-Xchange documentconverter 7.10.2-rev6
Open-Xchange readerengine 7.10.2-rev3

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 #5484. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

67871 CVE-2019-18846
CVSS: 6.5

67874 CVE-2019-18846
CVSS: 5.0

67931 CVE-2019-18846
CVSS: 5.0

67980 CVE-2019-18846
CVSS: 5.0

68136 CVE-2019-9853
CVSS: 7.7

68252 CVE-2019-18846
CVSS: 5.0

68258 CVE-2019-18846
CVSS: 5.0

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 #5484.

66234 com.openexchange.usm.api.exceptions.OXCommunicationException: OX server returned error
A wrong check, in combination with a not updated sequence number led to the situation where a CalDAV client was re-creating change exceptions from the ”detached” part of a previously split event series.
Correctly check validity of recurrence identifiers, ensure to increment sequence number after series split.

67286 Need for extended debug logging to trace registration/unregistration of permanent

push listeners
Avoid loading context data when checking user validity.

68139 Google Calendar Abo can not be renamed after custom color was set for it
This was caused by bugs in googles reconfiguration code.
This has been fixed by adjusting google reconfiguration.

68181 Read emails are displayed in bold font independent of read/unread status on MacOS
On MacOS, the sender is always bold because it's easier to read with many rows and MacOS and iOS users are well trained by this style anyhow. Bold doesn't imply "unseen". In this case, however, there was also a little CSS bug. The date stayed gray for unseen messages; that's fixed. In addition, we set the sender now to extra-bold and dark black (#000) in order to have another visual decoration beyond the blue dot.

68219 Appsuite Middleware not logging provisioning actions
Caused by changed logging behavior in v7.10.x
This has been solved by changing log level to INFO and include effective schema strategy in log message.

68243 With Android appointment color and participants not displayed correctly after organizer change
Organizer was replaced by creator and organizer was excluded from list of participants.
List of participants contains now the organizer, organizer is not replaced by creator anymore.

68253 High CPU min. 3 Threads with >95% CPU in "WeakHashMap()"
DateFormatCache was not threadsafe.
This has been fixed by using a synchronized map.

68261 Follow up for appointments not possible on mobile
Was caused by missing backbone model.
This has been solved by adding Backbone model.

68346 IDN encoding incorrectly on send
Certain Hindi characters were dropped on Internet email address parsing.
This has been solved by maintaining Hindi characters on Internet email address parsing.

4 Changes relevant for Operators

4.1 Changes of Configuration Files

Change #SCR-572 New configuration option to append Hazelcast version to cluster group name dynamically
When performing a rolling upgrade of the middleware nodes in the cluster to 7.10.2 from a previous version (7.10.1 and earlier), the upgraded nodes will not join the Hazelcast cluster and fail to startup properly due to a change in the join process of the underlying Hazelcast library.
Therefore, a new configuration switch is introduced that takes care to dynamically append the Hazelcast version to the cluster name so that a new cluster group is created automatically for the upgraded nodes: com.openexchange.hazelcast.group.name.appendVersion
Please mind that this configuration property is only applicable for 7.10.2; later versions starting with 7.10.3 will always append the version identifier to the group name. The default value is false, so that there are no surprises when patching an existing 7.10.2 installation.
In summary, when planning the upgrade to 7.10.2 from an earlier release, com.openexchange.hazelcast.group.name.appendVersion should be set to true explicitly by the administrator.

4.2 Changes of Behavior

Change #SCR-571 Cluster group name extended with Hazelcast version identifier
In order to support rolling upgrade scenarios where the existing and updated middleware version ship with a different version of the underlying Hazelcast library, but will still use the same configuration settings, the group name that is used as identifier when joining a cluster gets extended dynamically with a version string referring to the version of the Hazelcast library. For example, in 7.10.3 that ships with Hazelcast 3.12.4, the group name configured through com.openexchange.hazelcast.group.name will be automatically extended with the suffix -3.12.4.
This will effectively prevent attempts to join an ”old” cluster of middleware nodes running on an earlier version.
Due to this change, the object name as used in MBeans registered by the Hazelcast framework will change accordingly. For example, when the group name is configured to ”oxmw”, the partition service’s MBean name would change from
`com.hazelcast:instance=_hzInstance_1_oxmw,name=_hzInstance_1_oxmw, type=HazelcastInstance.PartitionServiceMBean` to `com.hazelcast:instance=_hzInstance_1_oxmw-3.12.4,name=_hzInstance_1_oxmw-3.12.4, type=HazelcastInstance.PartitionServiceMBean`

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

66234, 67286, 68139, 68181, 68219, 68243, 68253, 68261, 68346, 67871, 67874, 67931, 67980, 68136, 68252, 68258,