



**Release Notes for Patch Release #5149**  
2019-03-13

**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

---

©2019 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of OX Software GmbH. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

## 1 Shipped Product and Version

Open-Xchange AppSuite backend 7.10.1-rev9  
Open-Xchange AppSuite frontend 7.10.1-rev9

Find more information about product versions and releases at [http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning\\_and\\_Numbering](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 #5133. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

**47790 CVE-2016-6849**  
CVSS: 7.1

**63411 CVE-2019-9739**

## 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 #5133.

### **63333 [L3] periodic Cleaners triggers update tasks**

Update process is triggered automatically when loading a context and context-associated DB schema has pending update tasks.

Solution: Do not trigger update if context is disabled.

### **63331 [L3] redirection if schemata is disabled**

In case context-associated server does not match the server associated with target node a CTX-0012 error is thrown, which initiates automatic redirection to another node (as configured through "com.openexchange.server.migrationRedirectURL" property).

Solution: Do not throw CTX-0012 error in case context is disabled to avoid automatic redirection to another node. Instead, outer logic recognizes that context is disabled through authorization service.

### **63135 Tasks not working correctly**

The reminder was not parsed properly since a recent change.

### **62835 [L3] Edit Copy Button in Draft folder does not work as expected for externally linked accounts**

The unified mail storage returned normal mail ids instead of unified ones for copy/move commands.

Solution: Return proper unified mail ids.

### **63216 [L3] update task fails: UPD-0014 Duplicate key name action**

UpdateTask was missing an index exists check.

Solution: Added an index exists check.

### **61388 [L3] Signatures not above quoted text**

If in 'Settings -> Mail -> Signatures' the option "Add signature above quoted text" is selected, the signature in forwarded mail is not above, it's placed at the bottom of mail.

Solution: Added "com.openexchange.mail.forwardUnquoted" setting to JSlob under path

"io.ox/mail//forwardunquoted" and use different 'selector' in forwarding context when mail are forwarded unquoted.

**63184 [L3] Recipient disappears if double-clicked then click away**

Bundling original tokenfield file (static) lead to loading it's content twice and custom 'prototype' fixes in our tokenfiled.js was overwritten by the second load.

Solution: Clean up bundle.

**62216 [L3] Task section > progress bar doesn't work on Chrome, Opera and Safari**

CSS background-size's implicit height value 'auto'.

Solution: Use 100% as value for height.

**63240 [L3] cannot open newsletters with new google chrome 72**

Links opened by blankshield are blocked due to security reasons.

Solution: Open links with rel="noopener" directly in chrome 72 and above. Note that this is just an intermediate fix and will be replaced as soon as the issue is fixed in blankshield.

**62970 Display Name incorrect in calendar event**

Fallback name was html encoded.

Solution: Use available attendee data as fallback.

## 4 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.

## 5 Fixed Bugs

63333, 63331, 63135, 62835, 63216, 61388, 63184, 62216, 63240, 62970, 47790, 63411,