



Release Notes for Patch Release #3358

July 4, 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

©2016 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of Open-Xchange AG. 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 7.6.3-rev13

Open-Xchange AppSuite frontend 7.6.3-rev14

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 #3315. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

46630 CVE-2016-5741

CVSS: 3.7

46688 CVE-2016-5740

CVSS: 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 #3315.

45113 "Please define at least one action"-Message not translated

New translation was added.

46563 Field position ignored when updating a filter rule

Position field was not used during an update.

This has been fixed by properly using position field during update.

46589 Inserting a mailfilter with position 0 and an empty list fails with BAD_POSITION Exception

It was not possible to create a filter rule with position 0.

Solution: Consider the rule position when adding a new rule.

4 Changes relevant for Administrators

4.1 Changes of Configuration Files

Change #3406 The '%sanitisedMessage' token has been introduced to the logback.xml in order to address the 'CVE-117: Improper Output Neutralization for Logs' vulnerability

<!-- The '%sanitisedMessage' token has been introduced in order to address the 'CVE-117: Improper Output Neutralization for Logs' vulnerability.

This token ensures that the 'LogSanitisingConverter' is used in the logging pipeline in order to sanitise log messages that might contain ESC sequences, something that could lead to log injection/tampering/forging. -->

```
<pattern>%date{"yyyy-MM-dd'T'HH:mm:ss,SSSZ"} %-5level [%thread]
```

```
%class.%method\(%class{0}.java:%line\)%n%sanitisedMessage%n%lmdc%exception{full}</pattern>
```

5 Tests

The Open-Xchange QA team has successfully verified all bug fixes that could be reproduced within a lab 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.

6 Fixed Bugs

45113, 46563, 46589, 46630, 46688,