



Release Notes for Patch Release #4964
2018-11-19

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

©2018 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 7.8.3-rev51
Open-Xchange AppSuite frontend 7.8.3-rev45
Open-Xchange Documentconverter-api 7.8.3-rev7

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 #4861. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

60089 CVE-2018-18462
CVSS: 5.4

60088 CVE-2018-18462
CVSS: 5.3

60025 CVE-2018-18463
CVSS: 4.8

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 #4861.

60889 Provisioning calls do not always consider server name/ID when looking up contexts
Missed possibility to check if a context exists in a certain server.
This has been solved by adding possibility to check a context's existence in the scope of the registered server, in which the called provisioning node is running in. Thus the client is able to check before-hand, in which setup a context exists.

60828 Segmented updates doesn't work with multiple domains
The feature has been designed to only serve one migrationRedirect URL.
This has been solved by adding the possibility to configure the migrationRedirectURL on a per-host base via the as-config.yml

60826 Sharing is not fully capable to deal with "segmented updates"
The LOCATED_IN_ANOTHER_SERVER exception was not properly handled in the ShareServlet.
This has been fixed by handling the exception properly, i.e. redirect the client to the appropriate node. Introduced a new migrationRedirectURL property for the ShareServlet to use in order to send a redirect to the correct node.

60455 Object doesn't support property or method 'from' with mailto link with IE11
Code minifier broke the sanitizer plugin.
This has been fixed by upgrading the code minifier to a newer version.

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

60889, 60828, 60826, 60455, 60089, 60088, 60025,