Release Notes for Patch Release #4049

April 3, 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 7.8.2-rev30
Open-Xchange AppSuite frontend 7.8.2-rev25
Open-Xchange Office 7.8.2-rev8

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 #4015. 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 #4015.

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.

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.

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.

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.

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   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.

5   Fixed Bugs

52235, 52157, 52151, 51462, 51399, 51222, 49236, 52255, 51863, 51667, 51622,