Release Notes for Patch Release #4393

2017-10-17

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 7.8.3-rev36
Open-Xchange AppSuite frontend 7.8.3-rev32
Open-Xchange AppSuite Office 7.8.3-rev11
Open-Xchange AppSuite Office-Web 7.8.3-rev10

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 #4376. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

55703 CVE-2017-15029
CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N)

55651 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55603 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55602 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55600 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55090 CVE-2017-13667
CVSS: 6.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:L)

55068 CVE-2017-13668
CVSS: 3.7 (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/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 #4376.

55409 Contact sort orders are inconsistent between ”address book” and ”select address dialog”
It was just sorted by the first character.
This has been fixed by adding recursion when letters are equal.

55362 Translation missing on upload timeout error
Missing string in i18n.
Added missing string to i18n, this is only the new string, the string itself is still not translated, the translation will be available with the next public patch.

55360 Potential XSS-Bug while handling Mail From
Possible control and/or white-space characters returned to clients.

This has been fixed by dropping control and/or white-space characters from E-Mail addresses.

55271 File name incorrect Japanese characters
Fullwidth digits were replaced in file names.
This has been solved by allowing fullwidth digits in file names.

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

55409, 55362, 55360, 55271, 55703, 55651, 55603, 55602, 55600, 55090, 55068,