



Release Notes for Patch Release #4131

2017-05-15

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

©2017 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 7.8.2-rev33
Open-Xchange AppSuite frontend 7.8.2-rev28
Open-Xchange Office 7.8.2-rev9
Open-Xchange Office-Web 7.8.2-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 #4112. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

53077 CVE-2017-8340

CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

53073 CVE-2017-8340

CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

52843 CVE-2017-8340

CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N)

52066 CVE-2017-8341

CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N)

52040 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)

3 Fixed Bugs

53077, 53073, 52843, 52066, 52040,