Release Notes for Patch Release #3626

October 24, 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

1 Shipped Product and Version

Open-Xchange AppSuite backend 7.6.2-rev61
Open-Xchange Documentconverter 7.6.2-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 bug fixes and changes that have been applied subsequently to shipping Patch Release #3568. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

47781 CVE-2016-6845
CVSS: 5.4

48843 CVE-2016-7546
CVSS: 3.1

49005 CVE-2016-8857
CVSS: 5.3

49014 CVE-2016-8857
CVSS: 5.3

49015 CVE-2016-8857
CVSS: 3.5

49155 CVE-2016-8857
CVSS: 2.0

49159 CVE-2016-8857
CVSS: 5.3

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 #3568.

46103 Not possible to send mail with more than one comma in senders name
Empty strings in splitAddrs method cause index out of bound exception.
This has been fixed by skipping empty strings.

47967 High CPU usage by Java process
An infinite loop while trying to determine a folder's reverse path to root folder caused the excessive creation of folder instances all kept in a wrapping java.util.ArrayList instance. It turned out that while loading the path for a folder from a subscribed external IMAP account, the special INBOX folder references itself as parent, consequently rendering the traversing loop infinite.
This has been solved by introducing several safety checks (in case a folder references itself as parent) and guards to prevent from possible such an infinite loop when trying to determine a folder's path to root folder.

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

46103, 47967, 47781, 48843, 49005, 49014, 49015, 49155, 49159,