Release Notes for Patch Release #4895

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

1 Shipped Product and Version

Open-Xchange AppSuite backend 7.6.3-rev43
Open-Xchange AppSuite frontend 7.6.3-rev35

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 #4860. 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<

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 #4860.

56912 Added \n after logout to signature
New/Missing line breaks after sanitizing.
This has been solved by do not pretty print signatures for OX6.

56001 Mail folder not loading: String index out of range
Possible 'java.lang.StringIndexOutOfBoundsException' while parsing an address list.
This has been solved by orderly reseting cached string length after string was modified.

53456 Mail content not displayed with broken content type
Corrupt/broken Content-Type header in a MIME part breaks parsing of a mail message.
This has been fixed by dealing with corrupt/broken Content-Type header when parsing a MIME part.

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

56912, 56001, 53456, 60089, 60088,