Release Notes for Patch Release #4790

2018-06-25

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 7.8.3-rev49
Open-Xchange AppSuite frontend 7.8.3-rev43
Open-Xchange Documentconverter 7.8.3-rev9
Open-Xchange Readerengine 7.8.3-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 #4744. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

58029 CVE-2018-9998
CVSS: 3.7

58051 CVE-2018-12610
CVSS: 3.7

58096 CVE-2018-9997
CVSS: 4.3

58161 CVE-2018-12611
CVSS: 4.3

58226 CVE-2018-12611
CVSS: 4.3

58256 CVE-2018-12611
CVSS: 5.4

58282 CVE-2018-12611
CVSS: 4.3

58874 CVE-2018-12609
CVSS: 6.5

58880 CVE-2018-12611
CVSS: 5.4

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 #4744.

58231 Extra blank line on each newline in signature
Replacing all new lines with br-tags caused long br-sequences.
This has been solved by not replacing newlines with br-tag, if signature looks like html.

4 Changes relevant for Operators

4.1 Changes of Configuration Files

Change #SCR-175 Added new property com.openexchange.server.migrationRedirectURL to server.properties
From the server.properties:

```
#Specifies the redirect URI/URL during cluster migration to which a client is redirected
in case it landed on a unsuitable node (running incompatible application code).
#E.g. a user gets routed to a node running application code in version X, but that account
has already been migrated to application code in version Y, e. g.: http://1.2.3.4
#No default value
com.openexchange.server.migrationRedirectURL=
```

Change #SCR-188 Changing readerengine.blacklist configuration regexp from file://.* to .* in order to block all (!) external Urls within document by default for security reasons
With the old setting, only file Urls to the local file system on the server were blacklisted. Since it would be still possible to access web services on the local system via external Urls within the document, the default has been changed to disallow all external Urls by default.
This strict setting has been chosen to forbid access to not allowed resources in a most secure way.

5 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.

6 Fixed Bugs

58231, 58029, 58051, 58096, 58161, 58226, 58256, 58282, 58874, 58880,