Release Notes for Patch Release #4791

2018-07-17

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 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 7.8.4-rev34
Open-Xchange AppSuite frontend 7.8.4-rev34
Open-Xchange Documentconverter 7.8.4-rev8
Open-Xchange Office-web 7.8.4-rev10
Open-Xchange Readerengine 7.8.4-rev5

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 #4771. 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 #4771.

58609 Incorrect translation for "Last name, First name"
Adjusted Translation to fix this issue.

58628 Attachment overlap for Print function
There was no styling for the print rendering.

This has been solved by adding a print rendering view.

58632 IE11: contact list view jump to different position when selecting a contact
Missing tabidnex messed up focus handling.
This has been fixed by adding tabindex -1 to labels for IE11.

58760 Usercopy fails with duplicate key
Usercopy failed with duplicate key.
Now 'target_id' for new reminder referenced the old object ID instead of the object ID for moved appointments/tasks.

58891 eMail address is not parsed correctly in text mails (when domain part contains a . and a -)
Was not mapped by regex.
This has been solved by adding both cases to this regex.

58905 Allow subnets for known proxies configuration
Changed behavior of com.openexchange.server.knownProxies: com.openexchange.server.knownProxies does now allow subnets as known proxies. Added SCR-49.

59401 Unable to Copy/ Paste in Chrome
A function for checking inline images did not expect non-html content and led to this non working Copy&Paste.
This has been solved by adjusting the check for inline images.

4 Changes relevant for Operators

4.1 Changes of Configuration Files

Change #SCR-49 Changed behavior of com.openexchange.server.knownProxies
com.openexchange.server.knownProxies does now allow subnets as known proxies. Changed description accordingly to:

- 192.168.1.50, 192.168.1.51
- 192.168.32.0/24, 192.168.33.36
- 192.168.32.0-192.168.32.255, 192.168.33.36
- 2001:db8:0:8d3:0:8a2e:70::/112
- 2001:DB8:0:8D3:0:8A2E:70:0-2001:DB8:0:8D3:0:8A2E:70:FFFF

A example list of know proxies in front of our httpserver/balancer as comma separated IPs and IP ranges.

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

58609, 58628, 58632, 58760, 58891, 58905, 59401, 58029, 58051, 58096, 58161, 58226, 58256, 58282, 58874, 58880,