Release Notes for Patch Release #4555

2018-02-07

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 7.8.4-rev22
Open-Xchange AppSuite frontend 7.8.4-rev20
Open-Xchange AppSuite office web 7.8.4-rev9
Open-Xchange AppSuite readerengine 7.8.4-rev4

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 #4538. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

56740 CVE-2018-5754
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

56718 CVE-2018-5755
CVSS: 7.7 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

56706 CVE-2018-5752
CVSS: 6.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:L)

56619 CVE-2018-5752
CVSS: 6.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:L)

56582 CVE-2018-5754
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

56580 CVE-2018-5754
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

56477 CVE-2018-5751
CVSS: 4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

56407 CVE-2018-5753
CVSS: 4.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

56359 CVE-2018-5756
CVSS: 4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

56334 CVE-2018-5752
CVSS: 6.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:L)

56333 CVE-2018-5756
CVSS: 4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

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 #4538.

56774 Copying users with individual filestores causes errors
When using the `usercopy` functionality for users which have individual filestores, unexpected errors were thrown. We resolved the situation in a way that errors during user copying are caught and handled correctly. We still deny copying users with individual filestores.

56496 Replying to HTML mail is using plain-text
On specific custom mail abstraction implementations, replying to HTML E-Mails lead to creation of plain-text E-Mails. This is related to the custom implementation and does not affect other operators. We added a workaround which needs to be validated at the target environment.

55894 Making `rampup` calls configurable for debugging
In certain environments the API `rampup` delivery inconsistent response times. We added debug logging if preconditions for this API exceed a specific threshold and added functionality to allow disabling those preconditions. Note that this serves solely to support debugging of actual issues and should not be used by default. See SCR-63 for more information.

55409 Inconsistent sort order at contact lists
Japanese sort order for contact lists at mail compose and the Contacts app were inconsistent. We updated the sort mechanism at those places to deliver consistent results.

4 Changes relevant for Operators

4.1 Changes of Configuration Files

Change #SCR-89 Added config switches for each ramp-up element
Added config switches for each ramp-up element to be able to enabled/disable a certain ramp-up operation. The `[client-id]` placeholder may hold the identifier of the client to which the setting applies; e.g. `open-xchange-appsuite`

- `com.openexchange.ajax.login.rampup.disabled.[client-id].serverConfig`
- `com.openexchange.ajax.login.rampup.disabled.[client-id].jslobs`
- `com.openexchange.ajax.login.rampup.disabled.[client-id].oauth`
- `com.openexchange.ajax.login.rampup.disabled.[client-id].folder`
- `com.openexchange.ajax.login.rampup.disabled.[client-id].folderlist`
- `com.openexchange.ajax.login.rampup.disabled.[client-id].user`
- `com.openexchange.ajax.login.rampup.disabled.[client-id].accounts`

Default value for each setting is `false`, which means the associated element is enabled.

Change #SCR-63 Track execution of individual calls issued by `rampup` request
Added property `com.openexchange.ajax.login.rampup.debugThresholdMillis`, which specifies the execution time threshold in milliseconds since when individual calls issued by rampup request are logged along-side with execution time in milliseconds.
This property requires `DEBUG` logging to be effective for class `com.openexchange.login.DefaultAppSuiteLoginRampUp` at `/opt/open-xchange/etc/logback.xml`.
If this property is not specified, every individual call will be logged. If a negative value is specified, logging is disabled. In case a positive value is specified, a call will only be logged if its execution time exceeds that threshold.

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 behaviour. Unless explicitly stated within this document, we do not expect any side-effects.

6 Fixed Bugs

56774, 56496, 55894, 55409, 56740, 56718, 56706, 56619, 56582, 56580, 56477, 56407, 56359, 56334, 56333,