Release Notes for Patch Release #4965

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.

1 Shipped Product and Version

Open-Xchange AppSuite backend 7.8.4-7-rev47
Open-Xchange AppSuite frontend 7.8.4-7-rev45
Open-Xchange Documentconverter-api 7.8.4-7-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 #4933. 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

60025 CVE-2018-18463
CVSS: 4.8

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 #4933.

61293 Moveuserfilestore inserts new entry in table filestore2user instead of updating the existing one
Wrong PRIMARY KEY specified for ”filestore2user” table, which allows duplicate entries per user.
This has been solved by avoiding duplicate entries in ”filestore2user” table when moving user’s file storage.

61128 Address displayed on one line if Contact map service setting is ”no link”
Css was broken.
This has been solved by adjusting CSS to display the address in multiple lines.

60889 Provisioning calls do not always consider server name/ID when looking up contexts
Missed possibility to check if a context exists in a certain server.
This has been solved by adding possibility to check a context’s existence in the scope of the registered server, in which the called provisioning node is running in. Thus the client is able to check before-hand, in which setup a context exists.

60455 Object doesn’t support property or method ’from’ with mailto link with IE11
Code minifier broke the sanitizer plugin.
This has been fixed by upgrading the code minifier to a newer version.

59528 MSG-0032 Categories=USER_INPUT Message=’Mail could not be found’
It was not possible to display messages fetched from IMAP having a corrupt BODYSTRUCTURE information.
More robust handling with IMAP messages having a corrupt BODYSTRUCTURE information solve this issue.

4 Changes relevant for Operators

4.1 Changes of Database Schema

Change #SCR-310 Fix PRIMARY KEY in ”filestore2user” table definition
PRIMARY KEY for ”filestore2user” table definition has been changed from ”PRIMARY KEY (cid, user, filestore_id)” to ”PRIMARY KEY (cid, user)” resulting in following table definition:

```
CREATE TABLE filestore2user (
cid INT4 UNSIGNED NOT NULL,
user INT4 UNSIGNED NOT NULL,
filestore_id INT4 UNSIGNED,
PRIMARY KEY (cid, user)
)
```

4.2 Changes of Commandline Tools

Change #SCR-308 Enhanced ”existscontext” command-line interface by a flag argument called ”inserver”
Enhanced ”existscontext” command-line interface by a flag argument called ”inserver”, which allows to control whether existence check should be limited to the registered server, with which the provisioning node is associated. Thus, if set true is only returned if both - such a context exists and is associated with the same server as the provisioning node.
How to use with existscontext: `--inserver - Whether check should be limited to the registered server this provisioning node is running in`

5 Changes relevant for Developers

5.1 Changes of internal APIs

Change #SCR-306 Enhanced plugin interface ”com.openexchange.admin.plugins.OXContextPluginInterface” by the method ”existsInServer”
Enhanced plugin interface ”com.openexchange.admin.plugins.OXContextPluginInterface” by the method ”existsInServer”, which is called whenever the corresponding ”existsInServer” method is called in ”com.openexchange.admin.rmi.OXContextInterface”.

Change #SCR-306 Enhanced plugin interface ”com.openexchange.admin.plugins.OXContextPluginInterface” by the method ”existsInServer”
Enhanced plugin interface ”com.openexchange.admin.plugins.OXContextPluginInterface” by the method ”existsInServer”, which is called whenever the corresponding ”existsInServer” method is called in ”com.openexchange.admin.rmi.OXContextInterface”.

5.2 Changes of provisioning APIs

Change #SCR-307 Added call ”existsInServer” to OXContextService SOAP end-point
Added call ”existsInServer” to OXContextService SOAP end-point, which allows to check if the specified context is associated with the same server (registered by ”registerserver” in the configuration database) as the called provisioning node. If true is returned, it is guaranteed that the context does exist and has the same server association.

6 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.

7 Fixed Bugs

61293, 61128, 60889, 60455, 59528, 60089, 60088, 60025,