Release Notes for Patch Release #4391

2017-10-17

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 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 7.6.3-rev32
Open-Xchange AppSuite frontend 7.6.3-rev27
Open-Xchange AppSuite Office 7.6.3-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 #4315. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

55703 CVE-2017-15029
CVSS: 3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N)

55603 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55602 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55600 CVE-2017-15030
CVSS: 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

55068 CVE-2017-13668
CVSS: 3.7 (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/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 #4315.

55162 Inline images at HTML mails disappear after a short time
Sometimes added Inline images disappeared while composing a new email.
Do not advertise "Content-Length" header for retrieved images from mail storage as associated MIME part does not provide exact size to solve this issue.

55360 Potential XSS-Bug while handling Mail From
Possible control and/or white-space characters returned to clients.
This has been fixed by dropping control and/or white-space characters from E-Mail addresses.

4 Changes relevant for Operators

4.1 Changes of Database Schema

Change #SCR-55 Added new ConfigDb tables for improved context provisioning
Added new ConfigDb tables for improved context provisioning;

```
CREATE TABLE contexts_per_dbpool (
db_pool_id INT4 UNSIGNED NOT NULL,
count INT4 UNSIGNED NOT NULL,
PRIMARY KEY (db_pool_id)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci;

CREATE TABLE contexts_per_filestore (
filestore_id INT4 UNSIGNED NOT NULL,
count INT4 UNSIGNED NOT NULL,
PRIMARY KEY (filestore_id)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci;

CREATE TABLE contexts_per_dbschema (
db_pool_id INT4 UNSIGNED NOT NULL,
schemaname VARCHAR(32) NOT NULL,
count INT4 UNSIGNED NOT NULL,
creating_date BIGINT(64) NOT NULL,
PRIMARY KEY (db_pool_id, schemaname)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci;

CREATE TABLE dbpool_lock (
db_pool_id INT4 UNSIGNED NOT NULL,
PRIMARY KEY (db_pool_id)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci;

CREATE TABLE dbschema_lock (
db_pool_id INT4 UNSIGNED NOT NULL,
schemaname VARCHAR(32) NOT NULL,
PRIMARY KEY (db_pool_id, schemaname)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci;
```

4.2 Changes of Command Line Tools

Change #SCR-57 Extended Context SOAP interface by 'checkcountsconsistency'
Additional 'checkcountsconsistency' added to available command-line tools.

5 Changes relevant for Developers

5.1 Changes of the RMI API

Change #SCR-56 Extended Context RMI interface by 'checkcountsconsistency'
Interface 'com.openexchange.admin.rmi.OXContextInterface' is extended by method 'checkCountsConsistency()' which ensures entries of count tables are consistent.

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

7 Fixed Bugs

55162, 55360, 55703, 55603, 55602, 55600, 55068,