# Release Notes for Patch Release #3629

October 24, 2016

## 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 7.8.1-rev24
Open-Xchange AppSuite frontend 7.8.1-rev22
Open-Xchange documentconverter 7.8.1-rev9
Open-Xchange EAS 7.8.1-rev11

Find more information about product versions and releases at `http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering`

# 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 #3571. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

**47781 CVE-2016-6845**
CVSS: 5.4

**48843 CVE-2016-7546**
CVSS: 3.1

**49005 CVE-2016-8857**
CVSS: 5.3

**49014 CVE-2016-8857**
CVSS: 5.3

**49015 CVE-2016-8857**
CVSS: 3.5

**49155 CVE-2016-8857**
CVSS: 2.0

**49159 CVE-2016-8857**
CVSS: 5.3

# 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 #3571.

**47967 High CPU usage by Java process**
An infinite loop while trying to determine a folder's reverse path to root folder caused the excessive creation of folder instances all kept in a wrapping java.util.ArrayList instance. It turned out that while loading the path for a folder from a subscribed external IMAP account, the special INBOX folder references itself as parent, consequently rendering the traversing loop infinite.
This has been solved by introducing several safety checks (in case a folder references itself as parent) and guards to prevent from possible such an infinite loop when trying to determine a folder's path to root folder. 48347;Report -t oxaas-extended does not terminate;Potential race conditions, when multiple hazelcast nodes work on the same report. Marking contexts as done, not always works like expected.
Solution: Made the processes more robust and removed potential vulnerability.

### 48681 Mail not displayed correctly on Android

The mail contains two parts of type text/plain. The second part contains the greetings. USM handles only the first part for sending the mail in plain text format to the client (used by Android).
With this fix USM concatenates all text/plain parts together.

### 48748 Distribution list view inconsistent, saving such a list does not work

With this patch the translation for all languages were delivered.

### 49210 Marked mail(s) disappear when hitting # 1 key on Numpad

Appsuite using a shared keypress handler for the numpad key and the 'a'. In combination with ctrl or another special key all messages get selected. A missing check in archive action allowed to archive a message with the numpad key.
Now checking for 'a' key before archive.

### 49236 Huge amount of Mail folder could not be found on mail server messages for non-existing folders

The message for "Mail folder could not be found on mail server" were known, actually by design, but not expected to happen that often.
The fix just excludes the inbox from the obfuscation, to reduce the amount of error messages.

### 49249 Oxsysreport complains about line 163: //tmp/ox_support_infos-20161007-133821/commands/cat /proc/cpuinfo: No such file or directory

This has been solved by fixing a typo.

### 49304 Crash on all Groupware Nodes

A newly introduced login handler stored an user attribute on each login operation, and the corresponding cache invalidation event was distributed remotely throughout the cluster, which lead to an increased number of unnecessary events.
This has been updated by only updating user attribute if it actually was changed, skip cluster-wide invalidation.

## 4 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.

## 5 Fixed Bugs

47967, 48681, 48748, 49210, 49236, 49249, 49304, 47781, 48843, 49005, 49014, 49015, 49155, 49159,