



OX Guard Release Notes for Patch Release #3493

August 18, 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

©2016 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of Open-Xchange AG. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

1 Shipped Product and Version

Open-Xchange Guard 2.4.2-rev5

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 bugfixes and changes that have been applied subsequently to shipping Release 2.4.2. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

47878

CVSS: 6.5

47914

CVSS: 4.3

48080

CVSS: 4.3

3 Bugs fixed since previous Public Release

This section provides a summary of bugfixes and changes that have been applied subsequently to shipping Release 2.4.2.

47886 Authentication subkey used for encryption

In case a keypair contains public subkeys for the "authentication" purpose, this key might be used to encrypt a mail depending on the order of those subkeys. This has been corrected by checking that the subkey for "encryption" purposes is used.

47902 Incorrect subkey used for signatures

In case multiple subkeys were present at a keypair and a mail got encrypted and signed, the encryption key was used for signing as well. As a result signature validation could fail. This has been corrected by making sure only subkeys for "signing" are used for that purpose.

48100 Error when trying to re-set a user account

When resetting a users private password via the command-line, an error was thrown. This worked fine when users were executing that action via self-service. That command has been modified to support being called by a administrative account.

4 Tests

Open-Xchange has successfully verified all bug fixes that could be reproduced within a lab environment.

To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server setup 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.

5 Fixed Bugs

47886, 47902, 48100, 47878, 47914, 48080,