OX Guard
Release Notes for Patch Release #6116

2022-03-23

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.

Copyright notice

1   Shipped Product and Version

Open-Xchange Guard 2.10.6-rev6

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 #6107. Solutions for vulnerabilities have been provided for the existing code-base via Patch Releases.

GUARD-333   CVE-2022-26876
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 #6107.

GUARD-296   Guard does not retrieve Keys from "Advanced Mode"-only WKD Servers
Outdated RFC draft implementation.
This has been solved by updating key retrieval and serving logic to match up vim RFC draft v12.

4   Changes relevant for Operators

4.1   Changes of Configuration Files

Change #SCR-998   Updating OX Guard's WKS key discovery logic to match RFC draft v. 12
OX Guard partially implements the "OpenPGP Web Key Directory" RFC draft in order to serve and receive user's PGP keys. Some aspects of fetching and serving keys are now changed in order to match up with the latest version of the draft.
Receiving Keys: When fetching keys via WKS, OX Guard does no longer perform SRV DNS lookups to find the appropriate key-server host. Instead an "advanced" query and a "direct" query are implemented. As a result the configuration option com.openexchange.guard.keySources.trustLevel-WKSSRVDNSSECServer becomes obsolete and is removed.
Serving Keys: For serving keys via WKS the "openpgpkey" subdomain must be valid and point to the new "openpgpkey" endpoint: ProxyPass /.well-known/openpgpkey balancer://oxguard/openpgp-key

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

6 Fixed Bugs

GUARD-296, GUARD-333,