OX Abuse Shield
Release Notes for Release 2.4.0

2020-08-13

Copyright notice

1 General Information

Open-Xchange is pleased to announce the release of OX Abuse Shield v2.4.0.

OX Abuse Shield provides abuse-prevention for Web Applications (including Webmail), POP, and IMAP. It is integrated with both OX App Suite and OX Dovecot Pro to prevent login and authentica-tionabuse as well as protecting against brute-force attacks.

The goal of OX Abuse Shield is to detect brute forcing of passwords across many servers, services and instances, as well as enforce policy for authentication and authorization. In order to support the real world, brute force detection policy can be tailored to deal with ”bulk, but legitimate” users of your service, as well as botnet-wide slow-scans of passwords.

The OX Abuse Shield v2.4.0 provides the following main improvements and new features

- New wf_dump_entries tool to dump stats DBs to file
- Support for new ”forwarding” type in replication messages
- Support for Prometheus via the new /metrics REST endpoint
- Add Date, Last-Modified and Cache-Control headers to all responses
- Session-ID now logged for allow/report commands
- Improved logging to show line numbers for Lua errors

The OX Abuse Shield v2.4.0 provides the following bugfixes

- Fix duplicate command stats under some circumstances

The wforce-policy v2.4.0 provides the following main improvements and new features

- Debian Buster support
- Custom Lua hook to handle RBL matches

The wforce-policy v2.4.0 provides the following bugfixes

- Add userdb_plugins/allusers.lua to the built package
- initRedis() was sometimes called with incorrect no of args

The new wforce-replfwd 2.4.0 provides the following main improvements and new features

- Note that this is the initial release of replfwd. The version number is synced to that of wforce to make it easier to track compatibility etc.
- Replfwd is a daemon to forward replication messages and black/whitelist entries between wforce clusters

What’s New in General

Open-Xchange now provides more detailed overviews, data sheet and product guide, relating to new product major release. These can be found at https://www.open-xchange.com/portfolio/

whats-new/

Download and Installation

For further details about OX Abuse Shield installation, mandatory and optional packages, policies, please refer to the documentation provided:http://oxpedia.org/wiki/index.php?title=AppSuite:OX_Abuse_Shield

General Information – Please Note

Open-Xchange encourages administrators to regularly update to the latest available release. To ensure a stable and up to date environment please note the different versions supported. An overview of the latest supported Major, Minor and Public Patch Releases can be found in the OXpedia at: https://oxpedia.org/wiki/index.php?title=OXAbuseShield:Version_Support_Commitment

New wf_dump_entries Tool

New tool to dump the contents of Stats DBs for debugging purposes.`man wforce_dump_entries` for more information.

Forwarding Type in Replication Messages

Replication messages now have a `forwarding` flag, which is used to indicate when a message has been forwarded. This can be used to prevent forwarding loops.

Support for Prometheus Metrics

Both the wforce and trackalert daemons support native Prometheus metrics via the new /metrics REST API endpoint. This endpoint follows the format described https://prometheus.io/docs/instrumenting/exposition_formats/

The prometheus metrics deprecate the existing metrics functionality including the following console commands:

- `showPerfStats()`
- `showCommandStats()`
- `showCustomStats()`

as well as the following REST API endpoints:

- `/?command=stats`

The prometheus metrics include metrics for many components that were not previously instrumented, including:

- Redis statistics
- DNS Queries
- Whitelists and blacklists

New HTTP Response Headers

All HTTP responses now include the following headers:

- Last-Modified
- Date
- Cache-Control

Last-Modified and Date headers will always reflect the current date/time as seen by the wforce server.

Session-ID Logging

The allow and report logs will now contain session_id information.

Improved Logging for Lua Errors

The Lua wrapper code has been updated to provide better traceback information, including line numbers, for Lua errors. This helps when writing Lua policy that triggers a Lua exception.

Fix Duplicate Command Stats

Under certain circumstances, relating to EOF handling when sockets are closed, REST API command statistics would be double counted. This has been fixed by refactoring the EOF handling code.

Custom Lua hook to handle RBL matches

Previously the RBL policy supported RBL multi-zones, where different responses could match on a single policy. However that didn't allow different policy actions to be taken depending on the matched zone.

Now if you wish to handle the action for IPs matching RBL zones, you can do so by registering a custom Lua function.

Here is an example:

```
local function processRBLBlock(lt, ret_msg, match_zone, match_ip, config)
return -1, ret_msg, "Remote IP matches RBL", {rbl_zone = match_zone, match_ip = match_ip}
end
```

If delayWhitelisting is true, and the IP is on the whitelist, then even if you return -1, this will be overridden to 0.

See wforce_policy man page for more details, in the Section titled "RBLs".

Replfwd Daemon

See the replwd and replfwd.conf man pages for more information.

2 Shipped Product and Version

OX Abuse Shield v2.4.0-rev1

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/.