# Zimbra Releases/10.0.12

## Contents



## Zimbra Collaboration Daffodil 10.0.12 Patch Release

Release Date: **December 17, 2024**

## Things to know before you upgrade

## Important change for zimbraLowestSupportedAuthVersion

The enforcement of zimbraLowestSupportedAuthVersion level=2 has been reverted in the 10.0.13 patch release. Please refer to the Release Note Fixed Issues section for more details

# Changes to SOAP API

There are changes in ChangePassword SOAP API. Please refer to API reference documentation. If you have custom auth implementation with ChangePassword, please incorporate changes to support new API changes.

## IMPORTANT: Admin Account authentication now honors zimbraAuthFallbackToLocal when using external/custom authentication. See: https://blog.zimbra.com/2024/04/admin-account-authentication-now-honors-zimbraauthfallbacktolocal/

Check out the Security Fixes sections for this version of Zimbra Collaboration. Please refer to the **Patch Installation** steps for Patch Installation instructions. As always, you are encouraged to tell us what you think in the Forums or open a support ticket to report issues.

## IMPORTANT: Instructions to update Zimbra's onlyoffice repository for installing zimbra-onlyoffice package.

Please note that there is no change in the onlyoffice package. Add Zimbra's onlyoffice repository to the server before Zimbra Daffodil v10 installation/upgrade. These repos will be included bydefault in upcoming Zimbra Daffodil version.

`https://repo.zimbra.com/apt/onlyoffice`

`https://repo.zimbra.com/rpm/onlyoffice`

You must add your local repository to your RHEL/CentOS Configuration :

**Redhat**

RHEL7

```
$ cat > /etc/yum.repos.d/zimbra-onlyoffice.repo <<EOF
[zimbra-onlyoffice]
name=Zimbra Onlyoffice RPM Repository
baseurl=https://repo.zimbra.com/rpm/onlyoffice/rhel7
gpgcheck=1
enabled=1
EOF
```

RHEL8

```
$ cat > /etc/yum.repos.d/zimbra-onlyoffice.repo <<EOF
[zimbra-onlyoffice]
name=Zimbra Onlyoffice RPM Repository
baseurl=https://repo.zimbra.com/rpm/onlyoffice/rhel8
gpgcheck=1
enabled=1
EOF

rpm --import https://files.zimbra.com/downloads/security/public.key
yum --disablerepo=* --enablerepo=zimbra-onlyoffice clean metadata
yum check-update --disablerepo=* --enablerepo=zimbra-onlyoffice --noplugins
```

**Ubuntu**

UBUNTU18

```
$ cat > /etc/apt/sources.list.d/zimbra-onlyoffice.list << EOF
deb [arch=amd64] https://repo.zimbra.com/apt/onlyoffice bionic zimbra
deb-src [arch=amd64] https://repo.zimbra.com/apt/onlyoffice bionic zimbra
EOF
```

UBUNTU20

```
$ cat > /etc/apt/sources.list.d/zimbra-onlyoffice.list << EOF
deb [arch=amd64] https://repo.zimbra.com/apt/onlyoffice focal zimbra
deb-src [arch=amd64] https://repo.zimbra.com/apt/onlyoffice focal zimbra
EOF

apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 9BE6ED79
apt-get update
```

## IMPORTANT: Incase above steps are missed for Onlyoffice installation, following is the manual steps for installation.

- As root user run below commands: (assuming Zimbra is already installed)

```
$ wget -O /opt/zimbra/bin/zmonlyofficeinstall https://raw.githubusercontent.com/Zimbra/zm-core-utils/10.0.9/src/bin/zmonlyofficeinstall
$ chmod 755 /opt/zimbra/bin/zmonlyofficeinstall
$ /opt/zimbra/bin/zmonlyofficeinstall
```

### IMPORTANT: Zimbra OpenSSL with default FIPS Configuration

- Please be advised that, TLS 1.2 is the minimum supported version if FIPS is being used with OpenSSL 3.0. We recommend using Zimbra with strong TLS configuration for increased security. Please follow instructions in **Cipher-suites-wiki** to set correct ciphers as per current versions of openssl, nginx and postfix.
- From this patch going forward Zimbra OpenSSL will be configured to work with FIPS compliance enabled by default. You do not need to take any action, unless you run into issues, you can switch to the non-FIPS provider as follows:

- Run below commands to Enable/Disable FIPS providers on all servers.

Disable FIPS provider:

```
As root user run below commands

Take backup of openssl.cnf
cd /opt/zimbra/common/etc/ssl
cp openssl.cnf <backup-path>/openssl.cnf

Copy openssl-source.cnf file
cd /opt/zimbra/common/etc/ssl
cp openssl-source.cnf openssl.cnf

Verify that, FIPS provider is disabled:
Run below command and verify fips provider is not listed
/opt/zimbra/common/bin/openssl list --providers

As zimbra user run below commands
su - zimbra
zmcontrol restart
```

Enable FIPS provider:

```
As root user run below commands

Take backup of openssl.cnf
cd /opt/zimbra/common/etc/ssl
cp openssl.cnf <backup-path>/openssl.cnf

Copy openssl-fips.cnf file
cd /opt/zimbra/common/etc/ssl
cp openssl-fips.cnf openssl.cnf

Verify that, FIPS provider is enabled:
Run below command and verify fips provider is listed
/opt/zimbra/common/bin/openssl list --providers

As zimbra user run below commands
su - zimbra
zmcontrol restart
```

## Security Fixes

| Summary | CVE-ID | CVSS Score |
|---|---|---|
| An issue with encoded @import statements in <style> tags that allowed the loading of malicious CSS has been addressed. | | |
| SSRF vulnerability in the RSS feed parser that allowed unauthorized redirection to internal network endpoints has been resolved. | CVE-2025-25065 | |
| An SQL injection vulnerability in the ZimbraSyncService SOAP endpoint has been resolved. | CVE-2025-25064 | |
| A Cross-Site Scripting (XSS) vulnerability via crafted <img> HTML content in the Zimbra Classic UI has been fixed. LC attribute **zimbra_owasp_strip_alt_tags_with_handlers** introduced in previous patch is no longer required and has been removed. | CVE-2024-45516 | |
| A Cross-Site Scripting (XSS) vulnerability via crafted HTML content in the Zimbra Classic UI has been fixed. LC attribute **zimbra_owasp_strip_alt_tags_with_handlers** introduced in previous patch is no longer required and has been removed. | | |
| A vulnerability in the ChangePassword API has been fixed to require a valid auth token. | | |

## What's New

# Zimbra Connector for Outlook

- Enhanced logging by adding the following information - Outlook version, Outlook, and ZCO language selected by the user.
- The install/upgrade history for the ZCO versions is now maintained.

## Fixed Issues

## Zimbra Collaboration

- After upgrading to iOS 18, users with IMAP-connected accounts experienced slower search performance, which led to overall slowness. It happened due to an update in the query parameters. The issue has been fixed.
- Messages scheduled through the "Send Later" option were deleted if mailboxd service was restarted before the messages were sent. The issue has been fixed.
- "Send Later" scheduled messages disappeared without sending when using a nonexistent email address for "zimbraAllowFromAddress". The issue has been fixed.
- When creating an appointment, users intermittently faced a "null check" error. The issue has been fixed.

## Modern Web App

**General**

- Shared folders are now displayed only on user request in Settings, with improved labeling. Unnecessary exclamation warnings have to been removed to avoid confusion for users.

## Mail

- EML file importing is now working on Zimbra version 10.0.0 and above.

## Packages

The package lineup for this release is:

```
zimbra-patch                            ->  10.0.12.1733205023-2
zimbra-mbox-admin-console-war           ->  10.0.12.1732701825-1
zimbra-mbox-webclient-war               ->  10.0.12.1732702815-1
zimbra-common-core-jar                  ->  10.0.12.1733200545-1
zimbra-mbox-store-libs                  ->  10.0.12.1732856866-1
zimbra-zco                              ->  1945.1732881109-1
zimbra-modern-ui                        ->  4.40.2.1733127251-1
zimbra-modern-zimlets                   ->  4.40.2.1733127251-1
```

## Patch Installation

Please refer to below link to install 10.0.12:

Patch Installation

## Quick note: Open Source repo

The steps to download, build, and see our code via Github can be found here: https://github.com/Zimbra/zm-build


---

**Support**

Overview
Zimbra Support Offerings
Professional Services
User Help
Customer Support Portal

**Learn**

What is Zimbra?
Demos and Videos
Case Studies
About Us

**Community**

Forums
Documentation
Blog
Submit a ticket