Veille Technologique – Zimbra Collaboration (édition libre et sécurité)

Nov 27, 2026 · @Serge Martins

Sujet de la veille

Zimbra Collaboration est une suite de messagerie collaborative (courriel, agenda, contacts, webmail) très répandue dans l'éducation et les collectivités. Deux sujets dominent son actualité en 2026 : la disparition des binaires libres officiels, qui fait reposer l'édition FOSS sur la communauté, et une série de vulnérabilités activement exploitées.

En bref

Élément	Situation au 27/11/2026
Éditeur	Synacor
Version courante	Zimbra 10.1 « Daffodil » (10.1.20 et suivantes)
Édition libre	Code source publié, mais plus de binaires officiels depuis la version 9
Binaires communautaires	Maldua (zimbra-foss), UALinux
Systèmes supportés	Ubuntu 22.04 / 24.04, RHEL 8 / 9 et dérivés ; pas Debian
Alternative issue de Zimbra	Zextras Carbonio Community Edition

Édition libre : qui fournit les paquets ?

- **Synacor** ne publie que le code source de l'édition Open Source ; les paquets prêts à l'emploi sont réservés à l'édition Network (payante).
- **Maldua** compile et publie des builds FOSS de chaque version 10.1.x, y compris pour Ubuntu 24.04, généralement peu de temps après chaque correctif.
- **UALinux** propose aussi des builds 10.1.x et un support commercial.
- Conséquence pour l'administrateur : le rythme des correctifs dépend d'un tiers ; il faut suivre les annonces de Synacor **et** du fournisseur du build.

Actualité sécurité

Vulnérabilité	Type	Conditions	Statut
CVE-2026-73570 (CVSS 8.9)	Injection de commandes via SNMP	Paquet zimbra-snmp installé et `snmp_notify` activé	Corrigée en 10.1.20 (20/07/2026), divulguée le 13/08, exploitée activement, ajoutée au catalogue CISA KEV le 21/08 ; plus de 270 serveurs compromis
CVE-2025-66376	XSS stocké dans le webmail	Ouverture d'un message piégé	Exploitée par la campagne « ZimReaper » ; corrigée dans les versions 10.x récentes

Ces failles s'ajoutent à un historique chargé (CVE-2022-41352, CVE-2024-45519…) : Zimbra est une cible privilégiée des attaquants, notamment contre les administrations.

Alternatives

Solution	Point fort	Point faible
Zimbra Network Edition	Support éditeur, sauvegarde et mobilité avancées	Licence payante
Carbonio CE (Zextras)	Fork moderne et libre de Zimbra, interface récente	Architecture plus lourde
Postfix + Dovecot + Roundcube	Léger, standard, maîtrisé	Pas d'agenda partagé natif
Exchange Server SE / Microsoft 365	Intégration AD et Outlook	Coût, dépendance Microsoft

Recommandations

1. Installer uniquement la dernière 10.1.x (au minimum 10.1.20) et suivre les « Security Center » de Synacor.

2. Ne pas installer zimbra-snmp ; s'il est présent, désactiver `snmp_notify` et appliquer le correctif.
3. Rechercher des indicateurs de compromission sur les serveurs exposés avant l'août 2026 (webshells, comptes inconnus).
4. Ne jamais exposer la console d'administration (7071) sur Internet ; activer l'authentification à deux facteurs.
5. En lab SISR : Ubuntu LTS, build FOSS Maldua, et comparer avec Carbonio CE.

Sources

- Synacor — Zimbra Security Center et notes de version 10.1.20
- CISA — Known Exploited Vulnerabilities Catalog (CVE-2026-73570)
- Projet Maldua — github.com/maldua/zimbra-foss
- Zextras — Carbonio Community Edition