Veille Technologique – Serveur DNS sous Debian 13 (BIND 9)

Nov 27, 2026 · @Serge Martins

Sujet et enjeux

BIND 9 reste le serveur DNS libre de référence, mais c'est aussi l'un des logiciels les plus corrigés : ISC a publié une dizaine de failles en 2025-2026, dont un **empoisonnement de cache** en octobre 2025. Un serveur BIND sous Debian 13 n'est sûr que s'il est mis à jour et configuré en résolveur fermé avec validation DNSSEC.

Rubrique	Contenu
Thème	Serveur DNS libre sous Debian 13 avec BIND 9
Technologies suivies	BIND 9.18 / 9.20, DNSSEC, alternatives (Unbound, PowerDNS, Knot)
Contexte	Serveur `deb-dns01` (zone `sisr.lan`, relais vers DC01 pour `martinscie.lan`)
Bloc BTS SIO	SISR – services réseau, logiciels libres, cybersécurité
Période couverte	Octobre 2025 à novembre 2026

Versions et alternatives

Debian 13 fournit **BIND 9.20** (paquet de sécurité `1:9.20.26-1~deb13u1` en 2026) ; Debian 12 fournit BIND 9.18.

Logiciel	Rôle	Point fort
BIND 9	Autorité + résolveur	Le plus complet, référence des cours et des certifications
Unbound	Résolveur seul	Léger, sécurisé, validation DNSSEC par défaut
PowerDNS	Autorité (base de données) + résolveur séparé	Zones dans MySQL/PostgreSQL, API

Logiciel	Rôle	Point fort
Knot DNS	Autorité seule	Performances, signature DNSSEC automatique
DNS Windows	Autorité + résolveur	Intégré à l'Active Directory, DoH depuis 2026

Actualité sécurité 2025-2026

Date	Faille	À retenir
21 oct. 2026	CVE-2026-19630, 94300, 96888, 97313	Épuisement de ressources, corruption mémoire GSS-TSIG, arrêts liés à RPZ (BIND 9.20 jusqu'à 9.20.29)
22 juil. 2026	CVE-2026-11331, CVE-2026-11622	Contournement de règles RPZ ; mémoire d'un résolveur DNSSEC qui dépasse sa limite
20 mai 2026	CVE-2026-5946, CVE-2026-5947, CVE-2026-3039	Arrêt de `named` par requêtes forgées ; épuisement mémoire pour les BIND intégrés à un AD (GSS-API)
22 oct. 2025	CVE-2025-40778 (CVSS 8,6), CVE-2025-40780, CVE-2025-8677	**Empoisonnement du cache** par enregistrements non sollicités ou générateur aléatoire faible ; corrigé par DSA-6033-1

Presque toutes ces failles provoquent un déni de service (arrêt du serveur) ; celles d'octobre 2025 permettaient d'**injecter de fausses réponses** dans le cache d'un résolveur. La validation DNSSEC en limite l'effet.

Recommandations

- [ ] Installer les mises à jour de sécurité Debian dès leur parution (`unattended-upgrades`) et redémarrer `named` .
- [ ] Ne jamais laisser un **résolveur ouvert** : récursion limitée au LAN (`allow-recursion`).
- [ ] Garder `dnssec-validation auto` pour les noms Internet.
- [ ] Séparer si possible le serveur faisant autorité et le résolveur (limite l'impact d'un empoisonnement).
- [ ] Interdire les transferts de zone, ou les protéger par clé TSIG.

- [ ] Suivre la matrice des failles BIND d'ISC et les avis du CERT-FR.

Intérêt pédagogique (SISR) : écrire un fichier de zone (SOA, NS, A, CNAME, MX) montre le fonctionnement interne du DNS que la console Windows masque ; comparer avec DC01 illustre le choix libre / propriétaire.

Sources

- ISC – CVE-2025-40778
- ISC – CVE-2026-3039
- ISC – CVE-2026-5946
- ISC – CVE-2026-5947
- ISC – CVE-2026-11331
- ISC – CVE-2026-11622
- Centre canadien pour la cybersécurité – Bulletin BIND AV26-1072
- Debian – DSA-6033-1 (LWN)
- Debian Security Tracker – CVE-2025-40778