



# Procédure de correction PHP

## CVE-2026-109618 / CVE-2026-109619

### Version 1.0

|                           |                                             |
|---------------------------|---------------------------------------------|
| <b>Rédacteurs</b>         | Hervé HENOCH (Responsable technologie)      |
| <b>Référence</b>          | À attribuer                                 |
| <b>Nom du fichier</b>     | Procedure_correction_PHP_Edissyum_v1.0.docx |
| <b>Date</b>               | 22/10/2026                                  |
| <b>Version</b>            | 1.0                                         |
| <b>Statut</b>             | Validé                                      |
| <b>Prochaine révision</b> | À la prochaine faille PHP critique          |

#### Historique des versions

| Version | Date       | Auteur       | Nature           |
|---------|------------|--------------|------------------|
| 1.0     | 22/10/2026 | Hervé HENOCH | Version initiale |

## Objet

Cette procédure corrige les deux RCE critiques PHP du 21/10/2026 sur un serveur Debian, de l'inventaire à la preuve que le correctif tourne en mémoire.

Un serveur n'est corrigé que si les trois conditions sont réunies : le paquet installé est en version corrigée, chaque service PHP a été redémarré après la mise à jour, et aucun processus ne garde l'ancien code en mémoire. Un `php -v` à jour ne prouve rien à lui seul : il ne montre que le CLI.

Toutes les commandes se lancent avec un compte ayant sudo.

## 1. Inventaire

Relever l'OS, toutes les branches PHP installées et ce qui sert réellement le web.

```
hostname; cat /etc/issue
dpkg -l | awk '/^ii/ && $2 ~ /^(php[0-9.]+-common|libapache2-mod-php[0-9.]+)$/ {print $2, $3}'
ls /etc/apache2/mods-enabled/ | grep php
systemctl list-units --type=service --state=running | grep -i fpm
sudo grep -RnE 'php[0-9.]*-fpm|fcgi:|FCGIWrapper' /etc/apache2/sites-enabled/ /etc/apache2/conf-enabled/
update-alternatives --display php-cgi 2>/dev/null | head -3
```

| Ce qu'on cherche           | Où le lire                                                                         |
|----------------------------|------------------------------------------------------------------------------------|
| Branches installées        | <code>dpkg -l</code> : la version de chaque phpX.Y-common et libapache2-mod-phpX.Y |
| Source des paquets         | suffixe de version : ~debN = Debian ou Freexian, +0~AAAAMMJ... = Sury              |
| <code>mod_php</code> actif | le phpX.Y.load présent dans mods-enabled                                           |
| PHP-FPM utilisé            | les sockets phpX.Y-fpm cités par les vhosts                                        |
| php-cgi (ISPConfig, fcgid) | les FCGIWrapper et la cible de php-cgi                                             |

**Remarque :** `grep -R` en majuscule est obligatoire : les fichiers de sites-enabled sont parfois des liens symboliques, que `grep -r` ignore.

## 2. Choisir la source du correctif

La source dépend du couple OS / PHP : Freexian ne corrige que la version de PHP d'origine de chaque Debian, Sury couvre toutes les branches sur Debian 11 et 12.

| OS        | PHP | Source actuelle | Solution                    | Version corrigée attendue |
|-----------|-----|-----------------|-----------------------------|---------------------------|
| Debian 9  | 7.0 | Debian          | Freexian<br>ELTS<br>stretch | 7.0.33-0+deb9u26          |
| Debian 10 | 7.3 | Debian          | Freexian<br>ELTS<br>buster  | 7.3.31-1~deb10u16         |

| OS             | PHP           | Source actuelle | Solution                                           | Version corrigée attendue         |
|----------------|---------------|-----------------|----------------------------------------------------|-----------------------------------|
| Debian 11      | 7.4           | Debian          | Freexian ELTS bullseye ou Sury                     | 7.4.33-1+deb11u14 / 1:7.4.33-31   |
| Debian 11      | 7.4           | Sury            | Sury                                               | 1:7.4.33-31                       |
| Debian 11 / 12 | 8.2 à 8.5     | Sury            | Sury                                               | 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12 |
| Debian 12      | 8.2           | Debian          | Mise à jour Debian                                 | 8.2.35-1~deb12u1                  |
| Debian 9 / 10  | autre branche | Sury            | à vérifier avec apt-cache policy, sinon mitigation | à vérifier                        |

### 3. Préparer les dépôts

Lancer d'abord `sudo apt update` : ses erreurs indiquent lequel des cas ci-dessous traiter. Sauvegarder tout fichier avant de le modifier.

#### Sury : clé expirée (EXPKEYSIG B188E2B695BD4743)

La clé Sury a expiré le 04/02/2026 : les serveurs concernés ne reçoivent plus de mise à jour PHP depuis.

```
grep -rl sury /etc/apt/sources.list /etc/apt/sources.list.d/
ls /etc/apt/trusted.gpg.d/ | grep -iE 'php|sury'
curl -fsSLo /tmp/debsuryorg-archive-keyring.deb https://packages.sury.org/debsuryorg-archive-keyring.deb
sudo dpkg -i /tmp/debsuryorg-archive-keyring.deb
sudo apt-mark manual debsuryorg-archive-keyring
sudo rm /etc/apt/trusted.gpg.d/php.gpg
```

#### Remarques :

- Remplacer CODENAME par bullseye ou bookworm, et php.list par le nom trouvé au grep.
- Garder debsuryorg-archive.gpg : ce fichier est maintenu par le paquet.
- `apt-mark manual` empêche un autoremove de supprimer le trousseau.

#### Debian 9 / 10 : dépôts archivés

Buster et stretch ont quitté deb.debian.org et security.debian.org. Si sources.list y pointe encore, le remplacer (exemple buster) :

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.bak-$(date +%F)
```

```
sudo tee /etc/apt/sources.list > /dev/null << 'EOF'
deb http://archive.debian.org/debian/ buster main
deb http://archive.debian.org/debian-security buster/updates main
deb http://archive.debian.org/debian/ buster-updates main
EOF
```

**S'il pointe déjà vers archive.debian.org, ne pas le réécrire** : ajouter seulement la ligne manquante avec `tee -a` (souvent la ligne `-security`). Erreur Release file ... is expired : `sudo apt -o Acquire::Check-Valid-Until=false update`. Ligne bullseye-backports en 404 : la commenter.

## Freexian ELTS (Debian 9, 10, 11)

```
wget http://deb.freexian.com/extended-lts/pool/main/f/freexian-archive-keyring/freexian-archive-keyring_2022.06.08_all.deb
sudo dpkg -i freexian-archive-keyring_2022.06.08_all.deb
echo "deb http://deb.freexian.com/extended-lts CODENAME main contrib non-free" | sudo tee
/etc/apt/sources.list.d/freexian-elts.list
```

CODENAME = stretch, buster ou bullseye. Fichier introuvable : prendre le dernier keyring du même répertoire sur le site Freexian.

## Contrôle

```
sudo apt update
apt-cache policy phpX.Y-common | grep -E 'Installé|Candidat'
```

Le candidat doit correspondre à la version attendue de la section 2, sans erreur de signature.

## 4. Mettre à jour PHP

Mettre à jour uniquement les paquets PHP, toutes branches installées comprises.

```
sudo apt install --only-upgrade $(dpkg -l | awk '/^ii +(php[0-9]|libapache2-mod-php[0-9]|php-)/{print $2}')
```

Actions suite à cette commande :

- Relire le récapitulatif : aucune suppression, aucun paquet inattendu.
- Confirmer avec **O**. Sans confirmation, rien n'est installé.
- Question sur un php.ini modifié : répondre **N** pour garder la version locale.
- Les autres mises à jour système en attente se traitent à part, en fenêtre de maintenance.

## 5. Redémarrer les services

Un vrai redémarrage est obligatoire : un reload ou graceful d'Apache peut garder l'ancien `mod_php` en mémoire.

```
sudo systemctl restart apache2
for s in $(systemctl list-units --type=service --state=running --no-legend | awk '/php.*fpm/{print $1}'); do sudo systemctl restart "$s"; done
sudo pkill php-cgi # seulement s'il reste des php-cgi (fcgid les relance à la demande)
```

### Remarques :

- Toujours `sudo systemctl` : sans sudo, Debian 9 répond Failed to connect to bus alors que systemd fonctionne.
- Ne jamais faire un stop sans enchaîner le start : le site reste coupé.
- Contrôler que la ligne Active: affiche l'heure actuelle : `sudo systemctl status apache2 --no-pager | grep Active`.

## 6. Vérifier

Le serveur est corrigé quand les quatre contrôles passent.

```
dpkg -l | awk '/^ii/ && $2 ~ /^(php[0-9.]+-common|libapache2-mod-php[0-9.]+)$/ {print $2, $3}'
ls /etc/apache2/mods-enabled/ | grep php
sudo systemctl status apache2 --no-pager | grep Active
sudo sh -c 'for p in /proc/[0-9]*; do grep -qE " /(usr|lib|opt).*\((deleted\) $" $p/maps 2>/dev/null &&
cat $p/comm; done' | sort | uniq -c | sort -rn
zgrep -iE 'CVE-2026-10961[89]|bailout' /usr/share/doc/phpX.Y-common/changelog.Debian.gz
```

| Contrôle        | Résultat attendu                                                                                                                           |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Versions        | toutes les branches en version corrigée (section 2), y compris celle du module Apache actif                                                |
| Apache          | Active: à l'heure du redémarrage                                                                                                           |
| Mémoire (/proc) | ni apache2, ni php-fpm, ni php, ni php-cgi ; les autres services relèvent d'un redémarrage système                                         |
| Changelog       | les deux CVE ou <i>Avoid state corruption via bailout</i> (Freexian, Sury 7.x) ; pour Sury 8.x et Debian 12, le numéro de version fait foi |

**Le contrôle /proc doit se lancer avec sudo, sinon il est toujours vide.** Il ne voit que le code remplacé sur le disque : une branche jamais mise à jour n'y apparaît pas, d'où le contrôle des versions du module actif.

Terminer par un test dans le navigateur : connexion, ouverture d'un courrier, envoi d'un document.