Veille Technologique – xrdp et accès RDP Linux / Active Directory

Nov 27, 2026 · @Serge Martins

Sujet et enjeux

En 2026, xrdp a fait l'objet d'une vingtaine de CVE, dont une critique exploitable sans authentification. Debian 13 en fournit une version corrigée, alors qu'une faille reste ouverte sur Debian 12, passé en support LTS. Un serveur xrdp joint à l'AD doit donc être installé sous **Debian 13** et durci.

Rubrique	Contenu
Thème	Accès Bureau à distance (RDP) à des postes/serveurs Linux avec authentification Active Directory
Technologies suivies	xrdp / xorgxrdp, SSSD / realmd, Debian 12 et 13, alternatives RDP Linux
Contexte	Serveur `DEB-RDP01` sous Debian 13 dans l'infrastructure `martinscie.lan` (DC01, pfSense, VLAN Serveurs / Clients)
Bloc BTS SIO	SISR – Support et mise à disposition de services informatiques ; cybersécurité des services
Période couverte	Janvier à novembre 2026

Actualités récentes

La branche 0.9.x de xrdp (celle de Debian 12) est déclarée en fin de vie ; seule la branche 0.10.x est maintenue.

Date	Événement	Ce qu'il faut retenir
2026-07-12	Debian 12 passe en LTS	Fin du support de sécurité normal ; LTS jusqu'au 30 juin 2028, sur un sous-ensemble de paquets
2026-07-06	xrdp v0.10.6.1	Corrige 10 CVE supplémentaires et un plantage en TLS introduit par la 0.10.6

Date	Événement	Ce qu'il faut retenir
2026-04-17	xrdp v0.10.6	Corrige 8 CVE, dont CVE-2026-33145 et CVE-2026-32105 ; carte à puce désactivée par défaut
2026-01-28	xrdp v0.9.27	Dernier correctif 0.9.x ; les notes déclarent la branche 0.9.x en fin de vie
2026-01-27	CVE-2025-68670, corrigée en 0.10.5	Débordement de pile **sans authentification** dans le champ « domaine », exécution de code possible (CVSS 9.8). Corrigée par DSA-6123-1
2025-08-09	Sortie de Debian 13 « Trixie »	Embarque xrdp 0.10.1 et xorgxrdp 0.10.2

Point d'attention pour Debian 12 — CVE-2026-33145 : un utilisateur **authentifié** peut exécuter des commandes sur le serveur via le paramètre `AlternateShell` envoyé par le client RDP (actif par défaut). Debian ne corrigera pas bookworm (correctif jugé trop intrusif à rétroporter) ; trixie est corrigée en `0.10.1-3.1+deb13u2`.

Version de xrdp	Debian 12 (bookworm)	Debian 13 (trixie)
Paquet à jour	0.9.21.1-1+deb12u3	0.10.1-3.1+deb13u2
CVE-2025-68670 (non authentifiée)	Corrigée	Corrigée
CVE-2026-33145 (AlternateShell)	**Vulnérable, non corrigée**	Corrigée
Branche amont	0.9.x, fin de vie	0.10.x, maintenue

Solutions alternatives

xrdp reste la solution la plus simple pour un accès RDP multi-utilisateur avec l'AD via SSSD. GNOME Remote Desktop devient une alternative native, et Guacamole un complément pour un accès par navigateur.

Solution	Principe	Multi-utilisateur + AD	Version de référence	Limites
xrdp + xorgxrdp	Serveur RDP qui ouvre une session Xorg par utilisateur	Oui, via PAM/SSSD	0.10.6.1 (amont), 0.10.1 (Debian 13)	Pas de Wayland ; nombreuses CVE en 2026
GNOME Remote Desktop	Serveur RDP natif de GNOME, intégré à GDM en mode « connexion distante headless »	Oui : un identifiant RDP commun donne accès écran de connexion GDM, puis login AD	Fourni avec GNOME dans Debian 13	Impose GNOME ; mise en place plus délicate ; retours de bugs (écran noir, Kerberos) sur les forums
Apache Guacamole	Passerelle HTML5 : RDP/VNC/SSH dans le navigateur, sans client	Oui (extension LDAP/AD), mais se place **devant** xrdp	1.6.0 (juin 2025)	Composant de plus à maintenir (Tomcat + guacd)

Red Hat et SUSE documentent désormais GNOME Remote Desktop comme leur solution d'accès distant, signe d'une tendance de fond.

Impact pour martinscie.lan et recommandations

Le serveur `DEB-RDP01` est désormais installé sous **Debian 13** (xrdp `0.10.1-3.1+deb13u2`), qui corrige toutes les failles connues, dont CVE-2026-33145. Le guide d'installation Debian 13 intègre le durcissement ci-dessous.

À l'installation (Debian 13)

- [ ] Installer Debian 13 à jour : `apt update && apt full-upgrade`, vérifier `xrdp` en `0.10.1-3.1+deb13u2` ou plus récent.
- [ ] Dans `/etc/xrdp/sesman.ini` : `AllowRootLogin=false` et `AllowAlternateShell=false`.
- [ ] Forcer TLS dans `/etc/xrdp/xrdp.ini` : `security_layer=tls`.
- [ ] Réserver l'accès au groupe AD `GG_RDP_Linux` (`realm permit -g`).
- [ ] Limiter le port 3389 au VLAN Clients (pfSense et ufw), jamais exposé sur Internet.

En exploitation

- [ ] Suivre les avis DSA de xrdp et appliquer les mises à jour sans attendre.

- [ ] Surveiller le service `xrdp` et le port 3389 dans Zabbix.
- [ ] Évaluer Guacamole si un accès sans client RDP (navigateur) est demandé.

Les serveurs xrdp encore sous Debian 12 doivent être migrés : CVE-2026-33145 n'y sera pas corrigée, et le support LTS s'arrête le 30 juin 2028.

Outils et méthode de veille

Outil	Ce qu'il surveille	Comment s'abonner
Flux Atom GitHub xrdp	Nouvelles versions et CVE corrigées	Ajouter `https://github.com/neutrinolabs/xrdp/releases.atom` dans un lecteur RSS (Feedly, Inoreader, Thunderbird)
Debian Security Tracker	État des CVE par version de Debian	Page `security-tracker.debian.org/tracker/source-package/xrdp`
Listes debian-security-announce et debian-lts-announce	Avis DSA (Debian 13) et DLA (Debian 12 LTS)	Inscription sur `lists.debian.org`
CERT-FR (ANSSI)	Avis et alertes de sécurité en français	Flux RSS des avis sur `cert.ssi.gouv.fr`
NVD / CVE.org	Score CVSS et détail des vulnérabilités	Recherche par mot-clé « xrdp »

Rythme conseillé : lecture hebdomadaire du lecteur RSS, mise à jour de cette fiche à chaque nouvelle version de xrdp ou nouvel avis DSA/DLA.

Sources

- Notes de version xrdp (GitHub)
- Debian Security Tracker – xrdp
- Debian Security Tracker – CVE-2026-33145
- DSA-6123-1 – xrdp
- NVD – CVE-2025-68670

- Debian – Bookworm transmise à l'équipe LTS
- Debian – informations sur Bookworm
- Paquets xrdp dans Debian
- GNOME Remote Desktop (GitHub)
- Red Hat – accès distant au bureau (RHEL 10)
- SUSE – GNOME Remote Desktop (SLES 16.1)
- Apache Guacamole