DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 10-11-2026

BULLETIN ALERTES

Object	Vulnérabilité dans OpenSSH (sshd) sur Alpine Linux
Réference	1510
Date de Publication	2026-11-05
Sévérité	Elevé

IMPACT :

- Contournement de l'authentification par mot de passe
- Accès non autorisé à distance, sans authentification préalable

SYSTÉME AFFECTÉ :

- OpenSSH (sshd) versions antérieures à 10.6p2 sous Linux, lorsque le serveur est construit avec la bibliothèque musl sans PAM
- Alpine Linux, paquet openssh-server (sans PAM) ou openssh-server-pam avec UsePAM no, dans les versions antérieures aux versions corrigées listées dans la section SOLUTION

DÉSCRIPTION :

Une vulnérabilité a été identifiée dans le serveur sshd d'OpenSSH lorsqu'il est exécuté sans PAM sur un système Linux utilisant la bibliothèque musl, notamment Alpine Linux. Un attaquant distant peut se connecter à un compte sans mot de passe en soumettant un mot de passe de 257 à 1024 octets, à condition que la configuration le permette : l'authentification par mot de passe doit être activée, et au moins un compte local doit disposer d'un condensat de type 5 ou 6. Les images cloud Alpine 3.18.11 à 3.24.3 qui embarquent l'utilisateur alpine sans mot de passe sont concernées. L'éditeur n'indique pas d'exploitation active à ce jour.

SOLUTION :

Mettre à jour OpenSSH vers la version 10.6p2 (ou une version ultérieure) et, sous Alpine Linux, installer les versions corrigées du paquet openssh suivantes :

Alpine edge : 10.6_p2-r0 (ou une version ultérieure)

Alpine 3.24 : 10.3_p1-r2 (ou une version ultérieure)

Alpine 3.23 : 10.2_p1-r1 (ou une version ultérieure)

Alpine 3.22 : 10.0_p1-r11 (ou une version ultérieure)

Alpine 3.21 : 9.9_p2-r1 (ou une version ultérieure)

Alpine 3.20 : 9.7_p1-r6 (ou une version ultérieure)

Alpine 3.19 : 9.6_p1-r3 (ou une version ultérieure)

Alpine 3.18 : 9.3_p2-r4 (ou une version ultérieure)

Alpine 3.17 : 9.1_p1-r7 (ou une version ultérieure)

Alpine 3.16 : 9.0_p1-r6 (ou une version ultérieure)

Redémarrer le service sshd après la mise à jour, car l'installation du paquet ne remplace pas le démon en cours d'exécution. En l'absence d'application immédiate du correctif, Alpine Linux recommande de désactiver l'authentification par mot de passe (PasswordAuthentication no) puis de redémarrer sshd.

DOCUMENTATION :

Bulletins de sécurité OpenSSH et Alpine Linux

- https://www.openssh.org/releasenotes.html#10.6p2
- https://www.alpinelinux.org/posts/2026-11-05-openssh-password-authentication-bypass/

CVE-2026-123158 :

- https://www.cve.org/CVERecord?id=CVE-2026-123158