Alerte aux failles de sécurité pour PostgreSQL

Malgré ses qualités intrinsèques, l'outil de gestion des bases de données *open source* PostgreSQL (*« le secret le mieux gardé de l'*open source *»*, *sic*) n'est évidemment pas exempt de défauts. Les développeurs livrent ainsi aujourd'hui une mise à jour de sécurité pour cette offre, laquelle corrige trois failles, dont le niveau de criticité reste peu important.

« L'impact de ces trois problèmes sur la sécurité des serveurs est faible et le niveau de danger n'est pas alarmant, confirme **Damien Clochard**, directeur des opérations et cofondateur de la société Dalibo, spécialiste français de PostgreSQL. *Toutefois, nous recommandons fortement à tous les utilisateurs de PostgreSQL de mettre à jour leur installation. L'opération d'*upgrade *est simple et rapide, elle ne nécessite pas de validations applicatives, ni de tests de régression. La coupure de service induite par la mise à jour est donc très courte. »*

8.3, 8.4, 9.0 et 9.1

Ces trois vulnérabilités concernent respectivement le langage PL/python, les authentifications par certificat SSL et la gestion des fichiers de sauvegarde. Les moutures 8.3.18, 8.4.11, 9.0.7 et 9.1.3 de PostgreSQL corrigent ces différents problèmes. Notez que les développeurs ont profité de l'occasion pour éliminer d'autres bogues et instabilités. 45 correctifs sont ainsi appliqués à PostgreSQL 9.1.3.