

Thunderbird corrige ses bogues

Une nouvelle version de l'outil de communication (*e-mail*, flux RSS et *news*) *open source* Thunderbird vient d'être dévoilée. Elle corrige [quatre vulnérabilités](#) dont trois sont critiques.

La mise à jour de l'application est donc vivement recommandée. Dans la plupart des cas, elle sera proposée aux utilisateurs de façon automatique, soit *via* le système de mise à jour intégré à l'application, soit par le biais des dépôts logiciels de certaines distributions Linux. Au besoin, vous pouvez télécharger cette nouvelle mouture [directement sur le site de Mozilla Messaging](#).

La première faille critique touche la librairie chargée de décoder les images au format PNG. Des problèmes dans la gestion de la mémoire peuvent mener à un plantage de l'application. Les pirates peuvent alors mettre à profit la corruption de mémoire engendrée afin d'exécuter du code distant sur la machine de l'utilisateur **et en prendre le contrôle**.

Les deux autres failles majeures concernent là encore des problèmes de plantage avec corruption de la mémoire. Toutefois, contrairement à ce qui est annoncé sur le site de Mozilla Messaging, **ces vulnérabilités ne sont que peu importantes**. De fait, elles ne sont exploitables qu'au travers du moteur JavaScript de Thunderbird. Or, les messages ne peuvent pas l'utiliser par défaut.

Critiques ou pas, ces failles sont maintenant corrigées. Aucun *'exploit'* n'ayant été diffusé, nous pouvons supposer que les machines sur lesquelles Thunderbird est installé n'ont pas été compromises.