

Bugzilla : une faille zero day révèle les bugs des logiciels

Le problème qui touche aujourd'hui le système de suivi des bogues **Bugzilla** est inédit. Le logiciel permet en effet d'afficher la liste des vulnérabilités non corrigées présentes dans une application. De quoi faciliter le travail des pirates.

En principe les failles non comblées ne sont pas affichées publiquement, afin de ralentir leur exploitation (ou la mise au point d'un exploit). Seuls les développeurs du projet concerné en sont informés. Ce bug de Bugzilla, qui révèle publiquement les bugs de sécurité des logiciels, met donc à mal un grand nombre d'applications.

Correction de bogues pour Bugzilla

Lors de la procédure d'inscription sur une instance de Bugzilla, il est possible de passer outre la vérification de l'e-mail, et d'obtenir par ce biais certains droits étendus, en indiquant posséder une adresse e-mail utilisant le nom de domaine du projet.

Quatre failles de sécurité ont été éliminées dans les versions 4.0.15, 4.2.11, 4.4.6 et 4.5.6 de Bugzilla. La mise à jour de l'application devra être réalisée sans tarder, afin de se prémunir de ces vulnérabilités. Les versions suivantes de cet outil sont touchées :

- 2.23.3 à 4.0.14 (à remplacer par Bugzilla 4.0.15) ;
- 4.1.1 à 4.2.10 (à remplacer par Bugzilla 4.2.11) ;
- 4.3.1 à 4.4.5 (à remplacer par Bugzilla 4.4.6) ;
- 4.5.1 à 4.5.5 (à remplacer par Bugzilla 4.5.6).

Sur le même thème :

[Faille critique dans Xen : les Cloud d'Amazon et de Rackspace sont touchés](#)

[Un bug de Bugzilla divulgue 97 000 adresses e-mail de testeurs](#)

[Vol de mots de passe : Les hackers russes, Cybervor, en mode attaque ?](#)