Faille critique dans Xen : les Cloud d'Amazon et de Rackspace sont touchés

Une mise à jour de sécurité cruciale est aujourd'hui apportée à l'hyperviseur **Xen**. Le bulletin de sécurité XSA-108 vient d'être publié.

Il fait état d'une **faille critique sur des fonctions de bas niveau** : les MSR (*Model Specific Registers*) utilisés dans le cadre de l'émulation APIC (*Advanced Programmable Interrupt Controller*). En bref, l'émulation APIC définit l'accès à 256 MSR, alors que l'hyperviseur en simule 1024.

Conclusion, un programme mal intentionné peut aller lire des données qui vont au-delà de l'espace mémoire réservé par l'émulation APIC aux MSR. Les informations lues par ce biais peuvent être liées à d'autres machines virtuelles, voire à l'hyperviseur lui-même.

Toutes les versions de Xen à partir de la 4.1 sont concernées. Uniquement en mode x86 toutefois, les machines ARM étant épargnées. Il est à noter également que les OS fonctionnant en mode paravirtualisé ne sont pas impactés. Bref, seules sont touchées les machines virtuelles exploitant la virtualisation matérielle.

Notez qu'en mode paravirtualisé – une des spécificités de Xen –, l'OS s'adapte à l'hyperviseur, ce qui permet de ne plus avoir à émuler un PC complet. Cette technique permet d'améliorer les performances de la VM, mais nécessite un OS spécifiquement modifié en conséquence.

Amazon et Rackspace concernés

Les Cloud publics d'Amazon et de Rackspace sont touchés par cette faille de sécurité. Amazon a été exemplaire dans ce domaine, en **mettant en jour Xen avant la publication du bulletin de sécurité**, et en publiant des informations sur l'avancée de ses travaux. La semaine passée, **Jeff Barr**, *chief evangelist* AWS, donnait en effet la feuille de route du redémarrage des serveurs concernés par cette vulnérabilité (voir l'article « Amazon reboote son Cloud pour corriger Xen »).

La firme précise aujourd'hui que le redémarrage zone par zone des machines touchées s'est effectué comme prévu et dans les délais annoncés. Devant la possibilité qu'une telle action se reproduise dans le futur, Amazon livre ses conseils. Le premier est bien évidemment de suivre avec attention les alertes transmises par la société. Le second est de **répartir les machines virtuelles sur au moins deux zones différentes**. Elles ne redémarreront ainsi pas simultanément. Des fonctions de répartition de charge permettront alors de s'assurer que le service ne sera pas interrompu.

Rackspace a pour sa part été plus discret. L'opérateur de Cloud public a redémarré certains serveurs, dans l'urgence, et sans informer précisément ses clients sur les raisons de cette opération. Le patron de la firme s'excuse aujourd'hui, en expliquant qu'il ne souhaitait pas alerter les pirates sur le risque qui pesait sur le Cloud de la société. Un manque de transparence que tous n'apprécieront pas.

A lire aussi :

XenServer 6.2 : plus costaud, plus ouvert
Amazon renforce sa machine virtuelle Linux pour EC2
Rackspace choisit de ne plus se vendre

Crédit photo : © drx – Fotolia.com