Encore une faille critique dans l'hyperviseur Xen

Cela fait déjà plusieurs jours que le monde du Cloud s'agite autour d'une nouvelle vulnérabilité critique de l'hyperviseur Xen. De nombreux fournisseurs Cloud sont concernés : Amazon WS, Rackspace, IBM, Linode, etc…
Et ce n'est hélas pas la première fois qu'une faille extrêmement critique nécessite le redémarrage en urgence de l'hyperviseur Xen et donc le reboot de milliers de machine virtuelles. Le dernier problème similaire remonte seulement à septembre 2014 c'est à dire il y a moins de 6 mois (CVE-2014-7188).

Pour cette nouvelle faille, le correctif est disponible depuis plus de 10 jours. Les fournisseurs ont donc pu planifié son déploiement avec une certaine sérénité car ce n'est qu'aujourd'hui que les détails de la vulnérabilité (CVE-2015-2151) sont dévoilés et que d'éventuels Exploit pourraient voir le jour.
Pour les clients, l'impact aura été très variable selon le fournisseur Cloud. Pour certains CSP, le reboot systématique s'impose. Amazon avait annoncé dans un premier temps que seulement 10% des instances EC2 devraient rebooter. Finalement, Amazon a annoncé que grâce à leur Live update seulement 0,1% des instances AWS ont dû redémarrer.

Que risque-t-on si le fournisseur de Cloud n'applique pas le correctif ?
Pour cela, il suffit de lire la section « Impact » du bulletin de sécurité :
A malicious guest might be able to read sensitive data relating to other guests, or to cause denial of service on the host. Arbitrary code execution, and therefore privilege escalation, cannot be excluded.

En d'autres termes dans un Cloud public comme Amazon AWS, un locataire du service IaaS pourrait potentiellement réaliser un « hypervisor escape », c'est à dire accéder à des données dans une VM invitée voisine (i-e celle d'un autre client), faire un deni de service (arrêter des services), exécuter du code et éventuellement réaliser une élévation de privilège.

La faille est donc critique et prend une importance considérable dans un contexte de Cloud public. Il est donc important pour les clients de savoir quels sont les hyperviseurs utilisés par leurs fournisseurs et quels sont leurs engagements en matière de gestion des correctifs.

Autres ressources :

- Hypervisor memory corruption due to x86 emulator flaw
- Cloud : une faille Xen impose encore le reboot d’AWS, Rackspace et IBM