Patch Tuesday : des correctifs musclés sous pression de Hacking Team

Le piratage de la firme italienne Hacking Team continue de produire ses dommages collatéraux. Microsoft a certainement révisé à la hausse sa dernière livraison de correctifs de sécurité pour prendre en considération les derniers évènements. Le fameux Patch Tuesday comprend 14 bulletins de sécurité pour colmater 58 failles. Cette livraison comporte **4 bulletins classés comme critiques** touchant Internet Explorer et Windows.

Le bulletin MS15-065 corrige **28 failles dans IE** à partir de la version 6 jusqu'à la 11. Parmi ces vulnérabilités, on retrouve celle découverte dans le contenu piraté de Hacking Team. La firme italienne avait élaboré un POC avec une faille zero day dans IE. Le second bulletin critique, MS15-066, vise **le moteur VBScript** dans Windows Server 2003, Windows Server 2008 et Vista. Le troisième bulletin, MS15-067 , touche Windows 7 et 8 et cible **le protocole RDP**. Enfin, le quatrième bulletin, MS15-068, affecte les utilisateurs de Windows fonctionnant sur **Hyper-V**. Ils peuvent être amenés à télécharger un malware sur la machine virtuelle. Cette faille touche Windows 8, 8.1, et les versions de Windows Server 2008 et au-delà.

SQL Server corrigé et clap de fin pour Windows Server 2003

Les autres bulletins sont classés comme importants avec une mention spéciale pour le MS15-058 qui s'adresse à **SQL Server**. C'est assez rare de voir un correctif sur le serveur de base de données de Microsoft. Même estampillé comme important, ce patch permet l'exécution de code à distance et se classe donc dans les priorités à installer par les responsables IT. Les autres correctifs ciblent pêle-mêle Office et Windows.

Wolfgang Kandek, CTO de Qualys, note aussi que 9 des bulletins concernent Windows Server 2003. C'est la dernière fois que Microsoft publie des correctifs de sécurité pour cet OS. En effet, la fin du support est effective depuis le 14 juillet. Après les clients devront débourser 600 dollars par serveur pour obtenir les précieux bulletins de sécurité. Pour le responsable, il est urgent de migrer, car les cybercriminels vont certainement regarder attentivement les prochains Patch Tuesday pour déterminer les failles qui toucheront Windows Server 2003. Une technique déjà utilisée pour Windows XP.

A lire aussi :

Patch Tuesday : Colmatage renforcé pour IE et Office
Windows 10 signe la fin des Patch Tuesday sauf pour les entreprises

Crédit photo@mathiasmeisenthal-shutterstock