Microsoft Patch Tuesday : un bulletin de sécurité chargé en début d'année

Comme tous les seconds mardis du mois, Microsoft distribuera demain, mardi 10 janvier, son bulletin de sécurité, le premier de l'année 2012. Une diffusion qui tombe en fin d'après-midi, voire en début de soirée à l'heure européenne. Si l'on en croit le *« pre-patch tuesday »* de Redmond, ce nouveau bulletin sera beaucoup plus léger que celui qui a clos l'année 2011.

Mais janvier est généralement considéré comme un mois calme en matière de correctifs. On en comptait deux en 2011 et 2010 à la même période et un seul en 2009. Du coup, au final, ce bulletin de janvier 2012 et ses huit vulnérabilités, se présente comme un record.

La nouvelle édition du centre de sécurité de l'éditeur comprend sept bulletins. Soit moitié moins que les quatorze bulletins de décembre dernier. Plus inhabituel, seul un bulletin est estampillé comme « critique ». Non corrigées, les failles qui y sont référencées permettent l'exploitation de code à distance. Les six autres bulletins sont classés comme « importants » et permettront de corriger des risques d'élévation de privilèges, des contournements de sécurité, des risques de fuites d'informations voire des possibilités d'exécuter du code (malintentionné) à distance sur les machines infectées.

La catégorie des risques inclassables

Autre fait notable, toutes les alertes de Microsoft, à l'exception d'une, se concentrent sur des vulnérabilités de Windows, de XP à Windows Server 2008 R2 pour Itanium en passant par 7 et Server 2003, tant dans les versions 32 bits que 64 bits. Le bulletin numéro 7 visera à prévenir les vulnérabilités de l'outil Microsoft Developer Tools and Software. Autant de brèches de sécurité à combler dans les meilleurs délais.

À noter également l'introduction de *« Security Feature Bypass »* (SFB), une nouvelle classification des failles. Microsoft ne s'épanche pas sur cette innovation. *« SFB classe les problèmes qui ne peuvent pas être exploités directement, mais peuvent servir pour faciliter l'utilisation d'un autre exploit »*, se contente d'expliquer **Angela Gunn** sur le blog du Microsoft Security Response Center. En gros, une catégorie inclassable qui ne figurera pas forcément systématiquement dans les classifications habituelles de Redmond. À confirmer, ou non, le mois prochain.