

Microsoft Patch Tuesday de janvier : l'ombre de Meltdown et Spectre

Pour sa première tournée **Patch Tuesday** de 2018, **Microsoft** propose de colmater 56 vulnérabilités, dont 16 critiques (tout de même) dans un bundle dévoilé le 9 janvier.

Une large gamme de logiciels est concernée par la réactualisation: Internet Explorer, Microsoft Edge, Microsoft Windows, Microsoft Office, SQL Server, ChakraCore, .NET Framework, .NET Core, et ASP.NET. 28 d'entre elles permettent potentiellement d'exploiter du code à distance.

A ce [niveau d'information en package](#), on exclut les révélations portant sur les failles mémoires associées aux processeurs (Meltdown et Spectre) qui secouent l'écosystème IT global. Un update spécifique a été émis pour souligner le caractère atypique de l'alerte. D'autre part, Microsoft s'intéresse à la perte de performances des processeurs associés à Windows après instauration des patches. Et c'est [plutôt problématique](#) pour les configurations avec des anciennes générations de produits.

Néanmoins, dans une [contribution blog](#), Jimmy Graham, Directeur en charge des produits chez Qualys (fournisseur américain de solutions qui permet de scanner les systèmes en permanence pour dénicher les vulnérabilités), recommande de vérifier les bulletins suivant en lien avec Meltdown et Spectre : CVE-2017-5753, CVE-2017-5715, et CVE-2017-5754.

Avec Flash, Adobe demeure régulièrement liée à la sécurité Microsoft. C'est de nouveau le cas en ce début d'année.

Adobe a fourni sa propre liste de réactualisation logicielle mais la firme de Redmond insiste dans son Patch Tuesday sur le volet « critique » d'une vulnérabilité associée à Flash Player (alerte APSB18-01). Une vigilance qui s'adresse d'abord aux administrateurs qui reçoivent les updates Flash via Microsoft.

D'autres produits tiers sont concernés par le Patch Tuesday de janvier comme Mozilla Firefox, VMware, et Oracle.

Photo credit: [Yu. Samoilov](#) on [Visual hunt](#) / [CC BY](#)