Patch Tuesday : Patchwork de correctifs pour Office, IE et Windows

11 bulletins de sécurité dont 4 classés comme critique, pour 26 vulnérabilités corrigées : le **Patch Tuesday** d'avril 2015 est chargé et englobe un grand nombre de produits **Microsoft**.

Le premier bulletin (MS15-032) est aussi le plus dense. Classé critique et applicable à toutes les versions d'Internet Explorer de la 6 à la 11, il regroupe 10 failles, dont certaines critiques qui peuvent entraîner la prise de contrôle d'une machine à distance avec les privilèges de la session en cours.

L'une de ces vulnérabilités (CVE-2015-1661) est liée à l'implémentation du composant de sécurité ASLR. Le contournement de cette fonctionnalité du traitement aléatoire du format d'espace d'adresse peut permettre à des tiers de prévoir de manière plus fiable les décalages de mémoire d'instructions spécifiques dans une pile d'appels donnée. Il n'existe, selon Microsoft, aucun facteur atténuant.

Office et Windows touchés

Office n'est pas épargné par ce Patch Tuesday. Pas moins de 5 vulnérabilités, critiques sur certaines versions de la suite bureautique, sont regroupées dans le bulletin MS15-033. L'une des principales failles corrigées est liée à une corruption mémoire résultant du traitement de fichiers RTF.

Seules les versions les plus récentes de Windows (7, 8, 8.1 et Server 2008 R2/2012/2012 R2) sont concernées par le bulletin MS15-034, classé critique au regard du potentiel de la vulnérabilité CVE-2015-1635. Celle-ci se trouve dans la pile de protocole HTTP (HTTP.sys). Une solution de contournement a été identifiée, mais elle peut entraîner des problèmes de performances : désactiver la mise en cache du noyau IIS.

Egalement critique sur desktop (Windows Vista, Windows 7) comme sur serveur (Windows Server 2003/2008/2008 R2), le bulletin MS15-035 couvre la faille CVE-2015-1645. Cette dernière peut être exploitée à travers des fichiers de format d'image EMF (Enhanced Metafile) spécialement conçus… et que Windows traiterait de manière incorrecte.

Il existe une solution de contournement : désactiver le traitement des métafichiers en modifiant le registre. Problème : cette action peut entraîner une moindre qualité de l'apparence des applications ou des composants système… voire un dysfonctionnement total, selon ITespreso.

Du CVE à gogo

SharePoint Server 2010 et 2013 sont concernés par le bulletin MS15-036. Lequel corrige deux failles (CVE-2015-1640 et CVE-2015-1653) de type XSS (script inter-sites) exploitables lorsque SharePoint Server ne nettoie pas correctement une requête envoyée à un serveur.

Classé comme important, le bulletin MS15-037 couvre Windows 7 et Windows Server 2008 R2. Y est décrite la faille CVE-2015-0098, liée à la présence d'une tâche non valide dans le planificateur de tâches.

Pas un OS Windows encore supporté par Microsoft n'est épargné par les failles CVE-2015-1643 et CVE-2015-1644, colmatées dans le bulletin MS15-038. Toutes deux exploitent les erreurs engendrées quand Windows ne parvient pas à valider et à appliquer correctement les niveaux d'emprunt d'identité.

Le bulletin MS15-039 englobe Windows Vista et Windows 7, ainsi que Windows Server en versions 2003, 2008 et 2008 R2. Il corrige la faille CVE-2015-1646, liée au contournement de la fonctionnalité de sécurité de politique de source commune dans Microsoft XML Core Services (MSXML3).

Seul Windows Server 2012 R2 figure dans la liste rattachée au bulletin MS15-040, qui concerne la faille CVE-2015-1638. Des données peuvent être exfiltrées lorsque Active Directory Federation Services (ADFS) ne parvient pas à déconnecter correctement un utilisateur.

Tous les OS Microsoft encore pris en charge sont concernés par le bulletin MS15-041, relatif à la faille CVE-2015-1648. Cette dernière peut entraîner la divulgation d'informations lorsque ASP.NET traite de façon incorrecte certaines requêtes sur les systèmes sur lesquels les messages d'erreur personnalisés sont désactivés.

L'ultime bulletin (MS15-042) ne concerne que Windows 8.1 et Windows Server 2012 R2. Il couvre la vulnérabilité CVE-2015-1647, qui peut permettre un déni de service par exécution d'une application spécialement conçue dans une session de machine virtuelle.

A lire aussi :

Un Patch Tuesday musclé aux accents vintage
Patch Tuesday : IE et Windows à la fête, sauf Server 2003