

Adobe corrige une faille zero day de Flash

Adobe vient de livrer les derniers correctifs pour Flash de l'année 2015. Ce qui n'empêche pas l'éditeur de référencer ce bulletin ([APSB16-01](#)) comme le premier de l'année 2016. Trois semaines après la publication de la précédente vague de correctifs, la 32e de l'année, qui visait à combler [77 failles de sécurité](#), cette nouvelle prescription se contente d'alerter sur 19 vulnérabilités, dont certaines critiques. L'une d'entre elles étant même «*activement exploitée*» dans le cadre d'attaques ciblées, précise [l'Espresso.fr](#).

Il est vivement recommandé de télécharger, sur les systèmes Windows et Mac, la mise à jour 20.0.0.267 du plugin (18.0.0.324 pour la version bénéficiant du support étendu ; 11.2.202.259 sur Linux). Concernant les navigateurs, la mise à niveau se fera automatiquement sur Chrome, ainsi que sur Internet Explorer (Windows 8.x, Windows 10) et Edge (Windows 10) de Microsoft.

Faille zero day

La faille «*activement exploitée*» (CVE-2015-8651) hérite d'un score de criticité élevé : 8,8 sur 10 dans la dernière version de l'échelle CVSS («*Common Vulnerability Scoring System*»). Elle est liée à un problème de dépassement d'entier («*Integer Overflow*»), c'est-à-dire la représentation, lors d'une opération mathématique, d'une valeur numérique supérieure à celle représentable dans l'espace de stockage disponible.

Autre vulnérabilité particulièrement dangereuse : la CVE-2015-8644, qui peut permettre d'exécuter du code à distance via une confusion de type. En d'autres termes, l'accès à un objet en mémoire au travers d'une référence de type invalide afin de réaliser des opérations normalement interdites par la machine virtuelle. Les 17 autres failles sont liées à des problèmes de corruption de mémoire, notamment l'adressage de zones qui viennent d'être libérées («*Use-After-Free*»).

Une technologie dépassée

Les charges contre Flash se multiplient du fait de ces vulnérabilités qui composent autant d'opportunités de pénétration dans les systèmes informatiques. La tension est montée d'un cran avec le [piratage de Hacking Team](#). Une partie des documents dérobés à cette firme italienne présentée comme un «*mercenaire de l'ère digitale*» contribuant à l'espionnage d'Etat par voie électronique a fait la lumière sur les failles exploitées par les agences gouvernementales dans les principaux logiciels du marché... dont Flash.

Après Apple, qui a supprimé Flash d'iOS, Facebook est l'un des chefs de file de la contestation. Son directeur de la sécurité a invité Adobe à fixer une date pour la fin de vie de son plugin, afin que la transition vers HTML5 s'accélère. Pour montrer l'exemple, le réseau social a [banni Flash sur son lecteur de vidéos](#), privilégiant HTML5. La bascule a été progressive pour prendre en charge la compatibilité avec les plus anciens navigateurs.

Adobe travaille a la disparition de Flash

Du côté d'Adobe, la page Flash semble se tourner progressivement. Témoin ce renommage lourd de symbole annoncé début décembre : le logiciel d'animation Flash Professional est devenu Animate CC, après quasiment 20 ans d'exploitation commerciale. Plus efficacement peut-être, Adobe a également pris la décision de [fermer la page de téléchargement](#) de l'installateur Flash. Néanmoins, de part son plugin aujourd'hui massivement déployée sur les postes utilisateurs et la technologie toujours exploitée par un grand nombre de sites, la disparition de Flash nécessitera probablement encore quelques années...

Lire également

[Flash Player, cible préférée des kits de piratage](#)

[Google enterre les pubs Flash dans Chrome](#)

[Firefox fermera la porte aux plug-ins à la fin 2016](#)

crédit photo © drx - Fotolia.com