Faille Adobe Acrobat Reader : it’s not a bug, it’s a feature !

David Kierznowski, expert en sécurité informatique, a récemment publié article démontrant les risques engendrés par des fonctionnalités du logiciel Adobe Acrobat Reader. En effet, il serait possible de déclencher l’exécution de code arbitraire sans interaction avec l’utilisateur.

Techniquement, l’exploitation du défaut de sécurité est simple. Il s’agit de fabriquer un fichier PDF piégé contenant une URL vers laquelle sera automatiquement renvoyé l’utilisateur qui va ouvrir le document.

Dès lors, il est possible d’expédier l’internaute vers un site foisonnant de spywares, adwares et autres malwares? Sous le couvert d’un fichier PDF en apparence anodin, qui pourrait être envoyé par email ou déposé sur un site Internet légitime, l’utilisateur est à son insu redirigé vers un véritable nid de guêpes !

« Je ne considère pas vraiment ces attaques comme des vulnérabilités inhérentes à Adobe. Il s’agit plus d’exploiter des fonctionnalités du produit qui n’étaient pas conçues pour faire cela », explique David à notre confrère eWEEK.

David aurait découvert par moins de sept moyens d’injecter du code dans un fichier PDF. Il serait également possible, toujours à l’aide d’un PDF piégé, d’accéder aux ressources locales de la machine et notamment aux bases de données Adobe ADBC.

Adobe a bien pris note des découvertes du chercheur et planche en ce moment sur un correctif. Pour les plus techniques d’entre vous, n’hésitez pas à jeter un oeil sur le blog du chercheur dans lequel il explique ses trouvailles.