# Microsoft corrige une faille critique dans Internet Explorer

La mise à jour d'avril **d'Internet Explorer** reste encore une fois assez chargée, avec la correction de failles de sécurité présentes dans IE6, IE7, IE8, IE9, IE10 et IE11 (bulletin MS15-032).

Ces vulnérabilités permettent de lancer du code à distance, au travers d'une page web spécifique. Le pirate peut alors **prendre le contrôle de la machine de l'internaute**. La faille est d'une gravité très importante. Il faudra donc la combler sans délai, en installant le correctif proposé via Windows Update.

Notez que cette vulnérabilité est **classée critique** sur les OS desktops, mais seulement modérée sur les systèmes serveur. Si l'usage d'un navigateur web sous Windows Server demeure peu courant, nous sommes en droit de nous demander en quoi il demeure moins risqué pour l'utilisateur qui visitera une page web piégée. Dans le doute, considérez cette faille comme critique sur tous les OS.

## Fin du SSL 3.0… sauf pour les entreprises

Comme prévu et annoncé en février (voir l'article « Internet Explorer soigne sa sécurité »), Microsoft **désactive aujourd'hui le support du SSL 3.0**, jugé trop peu sécurisé.

Les entreprises pourront le réactiver, afin – par exemple – de maintenir la compatibilité avec certaines de leurs applications web. Microsoft suggère toutefois de basculer les serveurs et applications web vers des protocoles de sécurité plus solides, comme le TLS 1.2.

**À lire aussi :**
Microsoft renforce l'utilisation du HTTPS au sein d'Internet Explorer
Project Spartan débarque sur les smartphones Windows 10
Le prochain moteur de rendu HTML de Microsoft réservé à Project Spartan