Patch day de juin: 12 correctifs dont 8 critiques

En ce chaud mois de juin, Microsoft n'a pas fait les choses à moitié pour son bulletin de sécurité mensuel. Si les précédents 'patch day' étaient plutôt maigres, celui-ci ne contient pas moins de 12 correctifs, dont 8 critiques. Inutile donc de souligner le caractère important de cette mise à jour.

Patchs critiques Le premier correctif (MS06-021) corrige 8 vulnérabilités dans Internet Explorer (notamment dans la gestion des contrôles ActiveX)qui pourraient permettre l'exécution de code à distance. Windows 98, ME, 2000, XP et Server sont concernés. Le bulletin MS06-022 corrige une vulnérabilité dans le rendu des images ART qui pourrait permettre l'exécution de code à distance lors de l'utilisation d'Internet Explorer. Tous les Windows sont concernés. Le bulletin MS06-023 corrige une vulnérabilité dans JScript qui pourrait permettre l'exécution de code à distance lors de l'utilisation d'Internet Explorer. Tous les Windows sont concernés. Le bulletin MS06-024 corrige une vulnérabilité dans le lecteur Windows Media qui pourrait permettre l'exécution de code à distance. Windows Media 7.1 installé sur Windows 2000 Service Pack 4, Windows Media 9 installé sur Windows 2000 Service Pack 4 ou Windows XP Service Pack 1 et Windows Media 10 installé sur Windows XP Service Pack 1 ou Windows XP Service Pack 2 sont impactés. Le bulletin MS06-025 corrige plusieurs vulnérabilités dans le service Routage et Accès distant (RRAS) qui pourraient permettre l'exécution de code à distance. Tous les Windows sont concernés sauf 98, 98SE et ME. Le bulletin MS06-026 corrige une vulnérabilité dans le moteur de rendu graphique qui pourrait permettre l'exécution de code à distance. Seuls Windows 98, 98SE et ME sont impactés. Le bulletin MS06-027 corrige la fameuse vulnérabilité critique dans Word qui pourrait permettre l'exécution de code à distance. Toutes les versions de Word, d'Office et de Work Suite sont concernées. Word pour Mac est épargné. Le bulletin MS06-028 corrige une vulnérabilité dans PowerPoint qui pourrait permettre l'exécution de code à distance. Les versions Mac et PC sont impactées. **Patchs Importants** Le bulletin MS06-029 corrige une vulnérabilité dans Microsoft Exchange Server exécutant Outlook Web Access qui pourrait permettre l'injection de script. Le bulletin MS06-030 corrige une vulnérabilité dans Server Message Block qui pourrait permettre une élévation de privilèges. L'attaquant doit disposer d'informations d'identification valides pour ouvrir une session en local, précise l'éditeur. Le bulletin MS06-032 corrige une vulnérabilité dans TCP/IP qui pourrait permettre l'exécution de code à distance. **Patch Modéré** Enfin, le bulletin MS06-031 corrige une vulnérabilité dans l'authentification mutuelle RPC qui pourrait permettre l'usurpation d'une ressource réseau de confiance. Un utilisateur aurait besoin de se connecter à un serveur RPC malveillant pour qu'une usurpation ait lieu. Un attaquant n'aurait aucun moyen de forcer un utilisateur à se connecter à un serveur RPC malveillant. Windows 2000 Service Pack 4 est la seule version concernée.