Patch Tuesday de Microsoft : 8 bulletins, dont 5 critiques

L'ensemble de ces mises à jour corrige une majorité de vulnérabilité permettant l'éxécution de code à distance.

Le premier bulletin (**MS08-018**) concerne une vulnérabilité « critique » constatée dans Microsoft Project. L'ouverture d'un fichier Project spécialement conçu permettrait l'exécution de code distant..

L'attaquant pourrait prendre le contrôle du système touché, installer ou supprimer des programmes ou encore créer de nouveaux comptes administrateur.

Le bulletin **MS08-021**, s'attaque également à une vulnérabilité critique. La faille est située dans le GDI (bibliothèque graphique). Elle permet l'exécution de code distant si un utilisateur ouvre un fichier image EMF ou WMF spécialement conçu. Cette vulnérabilité permettrait une prise de contrôle du système visé et la création de compte disposant de droits administrateur.

Le troisième correctif critique (**MS08-022**) corrige une vulnérabilité signalée confidentiellement dans les moteurs *script* VBScript et JScript de Windows. L'exécution de code à distance permettrait à un attaquant de prendre le contrôle du système visé et également d'installer, de créer des programmes ou encore de créer des comptes disposant de droits administrateur.

Le quatrième correctif (**MS08-023**), également critique, corrige une vulnérabilité signalée confidentiellement dans un produit Microsoft. L'affichage d'une page Web sous Internet Explorer (IE) spécialement conçue permettrait l'exécution de code distant. La vulnérabilité aurait toutefois moins de conséquences sur les comptes à privilèges réduits que sur les comptes disposants de droits administrateur.

La dernière vulnérabilité critique (**MS08-024**) corrige une faiblesse signalée confidentiellement. L'ouverture d'une page Web spécialement conçue avec IE permettrait l'exécution de code arbitraire à distance. Toute comme la précédente, ce sont les comptes à privilèges qui seraient touchés. Les comptes administrateurs seraient toutefois plus atteints que les comptes à privilèges moins élevés.

Trois correctifs importants

Les correctifs importants sont au nombre de trois. Le premier correctif (**MS08-020**) corrige une vulnérabilité signalée confidentiellement. Exploitée par un tiers, cette vulnérabilité permettrait à un attaquant d'envoyer des réponses à des requêtes DNS. Cette manœuvre permettrait d'usurper du trafic ou de le rediriger.

Le deuxième correctif (**MS08-025**) important s'attaque à une vulnérabilité contenu dans le noyau Windows. Un assaillant local pourrait prendre le contrôle du système affecté et créer, modifier ou supprimer des données ou également créer de nouveaux comptes.

Le dernier patch (**MS08-019**) rectifie une vulnérabilité de Microsoft Office Visio. Cette faiblesse, permettant l'envoi de code à distance, permettrait à un attaquant de prendre le contrôle du

système visé. Là encore, l'attaquant pourrait créer ou supprimer des données, créer des comptes dotés de privilèges. Les comptes aux privilèges limités subiraient moins de dommages que les comptes administrateurs.

L'ensemble de ces correctifs est téléchargeable sur ce lien.