Patch day de juillet : Microsoft propose 6 correctifs pour 11 failles

L'éditeur vient de mettre à disposition de ses utilisateurs six correctifs de sécurité. Trois sont jugés « critiques », deux importants, et le troisième » modéré ». Ces patchs corrigent 11 vulnérabilités notamment dans Windows et Office.

En ce qui concerne les correctifs pour les failles **critiques**, la première concerne une vulnérabilité dans le logiciel **Excel.** Elle résout une vulnérabilité révélée publiquement et deux vulnérabilités signalées confidentiellement ainsi que d'autres problèmes de sécurité identifiés lors d'une étude menée par Microsoft.

Ces vulnérabilités autoriseraient l'exécution de code à distance lorsqu'un utilisateur ouvre un fichier Excel spécialement conçu. Les utilisateurs dont les comptes sont configurés avec des privilèges moins élevés sur le système subiraient moins d'impact que ceux qui possèdent des privilèges d'administrateur.

La deuxième mise à jour critique concerne une vulnérabilité dans **Windows Active Directory** qui autoriserait l'exécution de code à distance. Plus précisément, elle corrige une vulnérabilité liée aux implémentations d'Active Directory sur Windows Server 2000 et Windows Server 2003, qui permettraient l'exécution de code à distance ou une condition de déni de service. Les tentatives d'exploitation de cette vulnérabilité entraîneraient probablement un déni de service.

Sur Windows Server 2003, un attaquant doit disposer d'informations d'identification valides pour exploiter cette vulnérabilité. Tout attaquant qui parviendrait à exploiter cette vulnérabilité pourrait prendre le contrôle intégral du système affecté. Il pourrait alors installer des programmes, afficher, modifier ou supprimer des données ou créer de nouveaux comptes.

Enfin, le bulletin MS07-04 corrige trois vulnérabilités critiques. Deux de ces vulnérabilités favoriseraient l'exécution de code à distance sur les systèmes où le **.NET Framework** est installé. Une vulnérabilité permettant la divulgation d'informations sur les serveurs Web exécutant **ASP.NET**. Dans tous les cas d'exécution de code à distance, les utilisateurs dont les comptes sont configurés avec des privilèges moins élevés sur le système subiraient moins d'impact que ceux qui possèdent des privilèges d'administrateur.

Voilà donc pour les failles les plus critiques, mais Microsoft ne s'arrête pas là et l'éditeur propose également deux correctifs pour des vulnérabilités jugées « importantes. »

Le premier concerne **Microsoft Office Publisher** et corrige une vulnérabilité révélée publiquement. Elle permet l'exécution de code à distance si un utilisateur affichait un fichier Microsoft Office Publisher spécialement conçu. Cependant, l'exploitation de cette vulnérabilité nécessite une interaction avec l'utilisateur.

La deuxième corrige une vulnérabilité dans **Microsoft Internet Information Services** qui permet l'exécution de code à distance si un attaquant envoyait des requêtes URL spécialement conçues à une page Web hébergée par Internet

Information Services (IIS) 5.1 sur Windows XP Professionnel Service Pack 2 ne fait pas partie de l'installation par défaut de Windows XP Professionnel Service Pack 2. Un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait prendre le contrôle intégral du système affecté.

Pour conclure, Redmond nous offre un dernier correctif « modéré » concernant **le pare-feu de Vista**. Une vulnérabilité dans l'outil pourrait entraîner la divulgation d'informations. Cette mise à jour corrige une vulnérabilité signalée confidentiellement. Elle permet à un trafic réseau entrant non sollicité d'accéder à une interface réseau. Un attaquant pourrait potentiellement récupérer des informations sur l'hôte affecté.

Le téléchargement des correctifs peut s'effectuer à partir de ce lien.