

MAJ critiques: MacOS X et Linux RedHat

Entreprise

Quelques jours avant le bulletin mensuel de Microsoft, Apple publie sa mise à jour pour le système d'exploitation MacOS X. Ce 'Security Update', qualifié de critique corrige plusieurs vulnérabilités permettant des attaques locales ou distantes afin de créer un déni de service.

Le site spécialisé K-Otik nous explique que les failles se situent aux niveaux des programmes : Apache (DoS), CoreFoundation (Elévation des privilèges), IPSec (négociation d'une connexion non autorisée), Kerberos (exécution de code distant), lukemftpd (exécution de code distant par un attaquant identifié), OpenLDAP (mauvais cryptage des mots de passe), OpenSSH (directory traversal), PPPDialer (fichier de log non sécurisé), QuickTime Streaming Server (DoS), rsync (directory traversal), Safari (DoS), Safari (Iframe Injection), SquirrelMail (SQL Injection), et tcpdump (ISAKMP DoS). Les versions concernées sont: MacOS X 10.3.5, 10.3.4, MacOS X Server 10.3.5, 10.3.4, MacOS X 10.2.8 et MacOS X Server 10.2.8. Le patch est téléchargeable sur le site d'Apple. Dans le même temps, l'éditeur Linux RedHat a mis en ligne son troisième service pack entreprises destiné à son OS entreprise Linux 3. Qualifié de « hautement critique » par Secunia, ce service pack est destiné à RedHat Enterprise Linux AS 3, ES 3 et WS 3. Il corrige un certain nombre de vulnérabilités pouvant être exploitées par un pirate pour compromettre un système vulnérable. Le service pack est téléchargeable sur le site Red Hat Network.