Enquanto grande maioria das falhas de segurança exploradas com o OS X tenham origem em aplicativos de terceiros (alô Adobe Flash e Java), vez ou outra uma falha no próprio sistema é descoberta, para o desgosto de quem é fã da plataforma. Uma dessas falhas apareceu no final de semana e ela é consideravelmente séria: ela grava o login e senha de usuários em um arquivo de texto, completamente desprotegido.

A vulnerabilidade está restrita a algumas configurações específicas e foi relatada no começo do mês pelo pesquisador de segurança David Emery na lista Cryptome . Segundo ele, com a atualização 10.7.3 para o OS X a Apple ativou um log de debug para todo o sistema, que por algum motivo grava o login e senha dos usuários no próprio log, em texto puro. O pessoal do ZDNet acabou descobrindo
que um usuário da Apple já havia
relatado esse erro
no fórum da empresa há meses.

Ao que parece, a vulnerabilidade atinge sistemas em que o usuário usava a criptografia FileVault no seu HD antes de atualizar para o OS X Lion , atualizou para o OS X Lion e não está usando o FileVault 2. Nessas configurações, os arquivos protegidos não estão tão protegidos assim.

A pior parte vem agora: esse log está em uma área desprotegida, que pode ser acessada por qualquer pessoa com login do Mac em questão. Ou pior ainda, conectando o HD do Mac via Firewire. O log é mantido por apenas algumas semanas, então quem atualizou na época em que o update 10.7.3 foi liberado provavelmente tem mais senhas armazenadas do que quem fez a atualização ontem apenas.

Agora que boa parte do mundo já sabe que essa falha existe, é bem provável que a Apple liber e uma correção de segurança para tapar o buraco. Que não deveria estar lá para começar.

Fonte: http://tecnoblog.net/100736/os-x-lion-falha-senha/