

Debian fumble jeopardizes all sshd-equipped servers

As has been widely reported, the maintainers of Debian's OpenSSL packages potentially compromised the security of any sshd-equipped system used by administrators. Administrators may wish to purge authorized_key files of public keys generated on a Debian-based machine. Simply using a Debian-based machine to access a remote server via SSH would be a security risk. However, if the user copied a public key generated on a Debian-based system to a remote server, they could take advantage of the higher security offered by password-free logins, then attempt to brute-force the password. This is especially susceptible to brute-force attacks, especially if the user's name is easily guessed.