

MD5 for passwords

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00935.html>

- *From:* Ivan Voras <ivoras@xxxxxxxxxx>
 - *Date:* Mon, 30 Oct 2006 23:27:14 +0100
-

In light of (fairly recent) attacks on MD5, is it still safe enough to use in password hashing, for example in unix-passwd-like salted password hashes?

Related to this, how do attacks vary with the length of hashed string (pre-image)? I'd guess that longer documents more vulnerable, but is it true?

.