## [SECURITY] LSIDLogin() is insecure and can allow user impersonation

\* This is all horribly insecure, but its hard not to be

However it excels at that more than could ever be imagined.

If, say when LDAP authentication is used, and for new users, the usr-> password is known (eg "" or \*), then the validation used for the Isid cookie can be

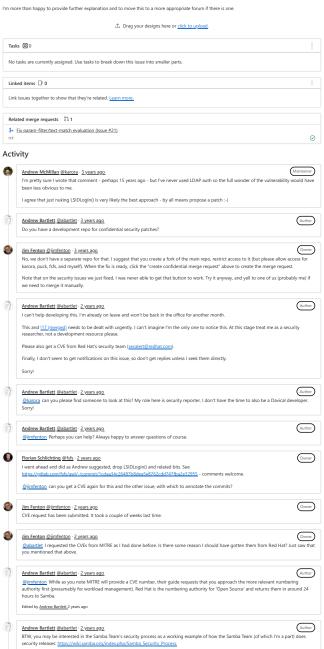
list( \$x, \$salt, \$y) = explode('\*', \$validation string); \$my\_validation = session\_salted\_md5(\$usr->user\_no . \$usr->username . \$usr->password, \$salt);

ontains only known or easily guessed inputs for this case. This is the case for user\_no, as this is a simple number and DaviCal (for example) displays it in an iternal page. Usernames are easily guessed and are likewise known to other users.

The salt should provide the security, but is is selected by the user, so the user can simply choose any value when computing their attack.

Finally, the whole design of the Isid cookie is flawed, there is no way to time out sessions, they last forever. This means that the logout relies on the browse being honest and destroying the cookie, there is no way to invalidate a cookie once issued, other than to change the password. Therefore if the cookie is stolen (eg JS XSS attack etc) then it can be re-used forever.

The fix should be to cut LSIDLogin() down to a no-op.



Andrew Bartlett @abartlet - 2 years ago @jimfenton In terms of Red Hat vs Mitre, it seems that has changed. Perhaps they got overwhelmed :-).

I certainly wouldn't wait 2 weeks for one however, and I think "Linux issues" is meant to mean "things found in a mainstream Linux distribution" (which DAViCal is) given how much the rest of the Open Source world has exploded.

Jim Fenton @imfenton - 2 years ago

Thanks, @abarrlet. I had seen Red Hat on the list of CNAs, but they're listed as "Linux issues only" and I interpreted that narrowly. Do you it's worth withdrawing that request and going to Red Hat?

Yes, please credit me as "Andrew Bartlett, Catalyst"

By the way. I presume it's OK to credit you as discoverer?

I don't want to be pushy, just figured it might be a useful reference.

