Software Vulnerabilities

Lewis Impey

Missing Authentication for Critical Function

This security vulnerability describes cases where the software does not perform any validation of the user’s identity before allowing access to privileged application functionality e.g. allow a user to add, modify or delete records without validating whether they are an admin or not.

The potential impact of this security vulnerability can depend on what functionality the software has, and can vary from trivial to severe. In the most severe of cases, its possible that private information could be disclosed or the entire application could be compromised.

To mitigated this software vulnerability, it is important that all functionality that uses privileged assets or information is identified. There should also be very clear roles defined for use within the application (such as admin and user) which have specific permissions given and withheld from them. It is also important to constantly check whether a user has access to the privileged information or assets that they are accessing.

Weak Passwords

This security vulnerability is rather straightforward, but a weak password is a password that is usually short, common, a system default (password is password) or something that could be very easily guessed with brute force attacks. Also passwords that could be guessed using a subnet that contains words from a dictionary, names, words based on the username, etc.

Since a password is a key to your computer (or another device/application) that could possibly contain very private information, it is important that a strong enough password is set so that it could not be easily guessed by someone trying to get into your account or device with malicious intent.

This is a very easy software vulnerability to fix, as it just entails changing a weak password to a stronger, more verbose password that is more difficult to guess. Below are some characteristics of a strong password that should be considered when creating a password:

* Contain both upper- and lowercase characters (e.g., a–z, A–Z).
* Have digits, punctuation characters, and letters (e.g., 0-9! (e.g., 0-9! @#$%^&\*()\_+|∼−=\′{}[]:“;'<>?,./).
* Are at least eight alphanumeric characters long.
* Not a word in any language, slang, dialect, jargon, etc.
* Are not based on personal information, names of family, etc.