**INADEQUATE FILE PROTECTION**

1. If folders and files lack appropriate protection (via user/group privileges etc.) then it becomes easy for a user to copy data from a network drive (for example) to their local system. The user could then copy that file to removable media, or send it out externally [1].
2. Access control involves the use of several protection mechanisms such as authentication (proving the identity of an actor) authorization (ensuring that a given actor can access a resource), and accountability (tracking of activities that were performed). When any mechanism is not applied or otherwise fails, attackers can compromise the security of the software by gaining privileges, reading sensitive information, executing commands, evading detection, etc. [2].
3. An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the system or network. Sensitive functionality should always be protected with access controls. However, configuring all but the most trivial access control systems can be very complicated and there are many opportunities for mistakes. If an attacker can learn of incorrectly configured access security settings, they may be able to exploit this in an attack. [3].

In applications, particularly web applications, access to functionality is mitigated by the authorization framework, whose job it is to map ACLs to elements of the application's functionality; particularly URL's for web apps. In the case that the administrator failed to specify an ACL for a particular element, an attacker may be able to access it with impunity. An attacker with the ability to access functionality not properly constrained by ACLs can obtain sensitive information and possibly compromise the entire application [4].

**REFERENCES**

1. <https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931>
2. <https://cwe.mitre.org/data/definitions/284.html>
3. <https://capec.mitre.org/data/definitions/180.html>
4. <https://capec.mitre.org/data/definitions/1.html>