# 6.2.2 Device Vulnerability Facts

A knowledgeable attacker can exploit network device vulnerabilities to gain access to network resources. Network device vulnerabilities include:

| Vulnerability | Description |
|---|---|
| Default Accounts and Passwords | Default accounts and passwords are factory defaults that already exist when a new network device is configured at installation. Default account names and passwords should be changed immediately when hardware or software is turned on for the first time. |
| Weak Passwords | Weak passwords are passwords that are blank, too short, dictionary words, or simple. In other words, they are passwords that can be quickly identified using password cracking tools. *Password cracking* is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.<br><br>Enforce complex passwords to reduce the risks of weak passwords. Complex passwords require passwords of a certain length (typically over 8 characters) and a mix of character types (numbers and symbols) along with requirements that the passwords are not words, variations of words, or derivatives of the user name. |
| Privilege Escalation | Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that aren't typically available to that user. Examples of privilege escalation include:<br><br>▪ A user accessing a system with a regular user account that is able to access functions reserved for higher-level user accounts (such as administrative features).<br>▪ A user who is able to access content that should only be accessible to a different user.<br>▪ A user who should only have administrative access that can access content that should only be available to a regular user.<br><br>Privilege escalation does *not* occur when a user is able to steal or hack administrator credentials and is therefore able to access administrative functions. Privilege escalation refers to accessing features with an account that normally should not have access to those features. |
| Backdoor | A *backdoor* is an unprotected access method or pathway. Backdoors:<br><br>▪ Include hard-coded passwords and hidden service accounts.<br>▪ Are often added during development as a shortcut to circumvent security. If they are not removed, they present a security problem.<br>▪ Can be added by attackers who have gained unauthorized access to a device. When added, the backdoor can be used at a future time to easily bypass security controls.<br>▪ Can be used to remotely control the device at a later date.<br>▪ Rely on secrecy to maintain security.<br><br>To protect against backdoors, do not allow programmers to bypass security during development. Carefully examine the code before release to remove any traces of backdoors that might have been included. |