Application Developer Considerations

If you are writing an application to read and write .ZIP files. Consider the following in your coding practices.

1. Path Traversal - The format defines storage locations for file and path locations. If you are reading a .ZIP file, make sure the code you write includes logic to avoid path traversal errors which could result in a malicious file being extracted that overwrites a valid system file, or other file. Check for conditions where a stored path may include a form such as ..\..\..\..\..\..\..\..\malicious_file.txt. The "dotted" paths in this file name could, if not accounted for within your application, extract and overwrite an important file.
2. Check sizes - when creating or reading a ZIP file, make sure you validate sizes for files and offsets as stored in the ZIP metadata fields. An incorrect, or malicious size could result in a system overload or application crash due to an unvalidated size that could exceed system or processing capacity.