


Prevent arbitrary file read via zip archives


A zip file with a file pointing to /etc/passwd would, upon being cleaned by mat2, produce a file with the filesystem's /etc/passwd file.

parent [e2c4dbf7](#)  master 

 No related merge requests found

 Pipeline [#96635](#) passed with stages - in 2 minutes and 13 seconds

Showing with 7 additions and 1 deletion

▼  **libmat2/archive.py** +7 -1

...	...	@@ -190,8 +190,14 @@ class ArchiveBasedAbstractParser(abstract.AbstractParser):
190	190	if member_name[-1] == '/': # `is_dir` is added in Python3.6
191	191	continue # don't keep empty folders
192	192	
193	-	zin.extract(member=item, path=temp_folder)
194	193	full_path = os.path.join(temp_folder, member_name)
	194 +	if not os.path.abspath(full_path).startswith(temp_folder):
	195 +	logging.error("%s contains a file (%s) pointing outside (%s) of its root.",
	196 +	self.filename, member_name, full_path)
	197 +	abort = True
	198 +	break
	199 +	
	200 +	zin.extract(member=item, path=temp_folder)
195	201	
196	202	try:
197	203	original_permissions = os.stat(full_path).st_mode
...	...	



[jvoisin](#) @[jvoisin](#) mentioned in issue [#174 \(closed\)](#) · 4 months ago

Please [register](#) or [sign in](#) to comment