

python / cpython Public

<> Code Issues 5k+ Pull requests 2.2k Actions Projects Security and q

Commit cf59bf7



encukou and StanFromIreland authored 9 hours ago · ✓ 94 / 97 · Verified

gh-146121: Clarify security model of pkgutil.getdata; revert checks (GH-148197)

This reverts commit [bcdf231](#), and clarifies get_data's security model.

Co-authored-by: Stan Ulbrych <stan@python.org>

main (#148197) · v3.15.0a8

1 parent [a4d9d64](#) commit cf59bf7

4 files changed +26 -27 lines changed

↑ Top ⚙️

Filter files...

- ✓ Doc/library
 - pkgtutil.rst
- ✓ Lib
 - pkgtutil.py
- ✓ test
 - test_pkgutil.py
- ✓ Misc/NEWS.d/next/Security
 - 2026-03-16-18-07-00.gh-issue-146121.vRbdro.rst

4 files changed +26 -27 lines changed

Search within code ⚙️

Doc/library/pkgutil.rst



@@ -151,24 +151,48 @@ support.

```

151 151      :meth:`get_data` <importlib.abc.ResourceLoader.get_data>` API. The
152 152      *package* argument should be the name of a package, in standard module
      format
153 153      (foo.bar). The *resource* argument should be in the form of a relative
154 - filename, using / as the path separator. The parent directory name
155 - .. is not allowed, and nor is a rooted name (starting with a /).
      154 + filename, using / as the path separator.
156 155
157 156      The function returns a binary string that is the contents of the specified
158 157      resource.
159 158
      159 + This function uses the loader method
      160 + ~importlib.abc.FileLoader.get_data
      161 + to support modules installed in the filesystem, but also in zip files,
      162 + databases, or elsewhere.
      163 +
160 164      For packages located in the filesystem, which have already been imported,
161 165      this is the rough equivalent of::
162 166
      163 167          d = os.path.dirname(sys.modules[package].__file__)
      164 168          data = open(os.path.join(d, resource), 'rb').read()
      165 169
      170 + Like the open function, !get_data can follow parent
      171 + directories (../) and absolute paths (starting with / or C:/,
      172 + for example).
      173 + It can open compilation/installation artifacts like .py and .pyc
      174 + files or files with reserved filenames <os.path.isreserved>.
      175 + To be compatible with non-filesystem loaders, avoid using these features.
      176 +
      177 + .. warning::
      178 +
      179 +     This function is intended for trusted input.
      180 +     It does not verify that *resource* "belongs" to *package*.
      181 +
      182 +     If you use a user-provided *resource* path, consider verifying it.
      183 +     For example, require an alphanumeric filename with a known extension, or
      184 +     install and check a list of known resources.
      185 +
166 186      If the package cannot be located or loaded, or it uses a loader

```

```

167 187     which does not support :meth:`get_data
      <importlib.abc.ResourceLoader.get_data>,
168 188     then None is returned. In particular, the :term:`loader` for
169 189     :term:`namespace packages <namespace package> does not support
170 190     :meth:`get_data <importlib.abc.ResourceLoader.get_data>.
171 191
192 +     .. seealso::
193 +
194 +         The :mod:`importlib.resources` module provides structured access to
195 +         module resources.
172 196
173 197     .. function:: resolve_name(name)
174 198

```



Lib/pkgutil.py



```

↑ ... @@ -393,9 +393,6 @@ def get_data(package, resource):
393 393     # signature - an os.path format "filename" starting with the dirname of
394 394     # the package's __file__
395 395     parts = resource.split('/')
396 -     if os.path.isabs(resource) or '..' in parts:
397 -         raise ValueError("resource must be a relative path with no "
398 -                            "parent directory components")
399 396     parts.insert(0, os.path.dirname(mod.__file__))
400 397     resource_name = os.path.join(*parts)
401 398     return loader.get_data(resource_name)

```



Lib/test/test_pkgutil.py



```

↑ ... @@ -61,25 +61,6 @@ def test_getdata_filesys(self):
61 61
62 62     del sys.modules[pkg]
63 63
64 -     def test_getdata_path_traversal(self):
65 -         pkg = 'test_getdata_traversal'
66 -
67 -         # Make a package with some resources
68 -         package_dir = os.path.join(self.dirname, pkg)
69 -         os.mkdir(package_dir)

```

```
70 - # Empty init.py
71 - f = open(os.path.join(package_dir, '__init__.py'), "wb")
72 - f.close()
73 -
74 - with self.assertRaises(ValueError):
75 -     pkgutil.get_data(pkg, '../.../etc/passwd')
76 - with self.assertRaises(ValueError):
77 -     pkgutil.get_data(pkg, 'sub/.../etc/passwd')
78 - with self.assertRaises(ValueError):
79 -     pkgutil.get_data(pkg, os.path.abspath('/etc/passwd'))
80 -
81 - del sys.modules[pkg]
82 -
83 64     def test_getdata_zipfile(self):
84 65         zip = 'test_getdata_zipfile.zip'
85 66         pkg = 'test_getdata_zipfile'
```



...6-03-16-18-07-00.gh-issue-146121.vRbdro.rst



[Load Diff](#)

This file was deleted.

Comments 0