python-pillow / **Pillow** Public

Code Issues 66 Pull requests 63 Discussions Actions Projects

Commit 9000313

radarhere and **wiredfool** committed on Feb 10 · 55 / 55

```
Fix OOB Write with invalid tile extents (#9427)

Co-authored-by: Eric Soroos <eric-github@soroos.net>
```

12.1.x · 12.1.1

1 parent cd01118 commit 9000313

9 files changed +53 -2

Top

Filter files…

- Tests
  - images
    - psd-oob-write-x.psd
    - psd-oob-write-y.psd
    - psd-oob-write.psd
  - test_file_psd.py
  - test_imagefile.py
- docs/releasenotes
  - 12.1.1.rst
  - index.rst
- src
  - decode.c
  - encode.c

Search within code

Tests/images/psd-oob-write-x.psd 1.1 KB

Binary file not shown.

Tests/images/psd-oob-write-y.psd 1.1 KB

Binary file not shown.

Tests/images/psd-oob-write.psd 36.3 KB

Binary file not shown.

Tests/test_file_psd.py

```
@@ -184,3 +184,20 @@ def test_layer_crashes(test_file: str) -> None:
184 184                 assert isinstance(im, PsdImagePlugin.PsdImageFile)
185 185                 with pytest.raises(SyntaxError):
186 186                     im.layers
    187 +
    188 +
    189 + @pytest.mark.parametrize(
    190 +     "test_file",
    191 +     [
    192 +         "Tests/images/psd-oob-write.psd",
    193 +         "Tests/images/psd-oob-write-x.psd",
    194 +         "Tests/images/psd-oob-write-y.psd",
    195 +     ],
    196 + )
    197 + def test_bounds_crash(test_file: str) -> None:
    198 +     with Image.open(test_file) as im:
    199 +         assert isinstance(im, PsdImagePlugin.PsdImageFile)
    200 +         im.seek(im.n_frames)
    201 +
    202 +         with pytest.raises(ValueError):
    203 +             im.load()
```

Tests/test_imagefile.py

```
@@ -169,6 +169,13 @@ def test_negative_offset(self) -> None:
169 169                 with pytest.raises(ValueError, match="Tile offset cannot be negative"):
170 170                     im.load()
171 171
+ 172     @pytest.mark.parametrize("xy", ((-1, 0), (0, -1)))
+ 173     def test_negative_tile_extents(self, xy: tuple[int, int]) -> None:
+ 174         im = Image.new("1", (1, 1))
+ 175         fp = BytesIO()
+ 176         with pytest.raises(SystemError, match="tile cannot extend outside image"):
+ 177             ImageFile._save(im, fp, [ImageFile._Tile("raw", xy + (1, 1), 0, "1")])
+ 178
172 179         def test_no_format(self) -> None:
173 180             buf = BytesIO(b"\x00" * 255)
174 181
```

docs/releasenotes/12.1.1.rst

```
@@ -0,0 +1,24 @@
+ 1  12.1.1
+ 2  ------
+ 3
+ 4  Security
+ 5  ========
+ 6
+ 7  :cve:`2021-25289`: Fix OOB write with invalid tile extents
+ 8  ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
+ 9
+ 10 Check that tile extents do not use negative x or y offsets when decoding or encoding,
+ 11 and raise an error if they do, rather than allowing an OOB write.
+ 12
+ 13 An out-of-bounds write may be triggered when opening a specially crafted PSD image.
+ 14 This only affects Pillow >= 10.3.0. Reported by
+ 15 `Yarden Porat <https://github.com/yardenporat353>`__.
+ 16
+ 17 Other changes
```

```
+ ==============
+
+ Patch libavif for svt-av1 4.0 compatibility
+ ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
+
+ A patch has been added to ``depends/install_libavif.sh``, to allow libavif 1.3.0
  to be
+ compatible with the recently released svt-av1 4.0.0.
```

docs/releasenotes/index.rst

```
@@ -15,6 +15,7 @@ expected to be backported to earlier versions.
   :maxdepth: 2

   versioning
+   12.1.1
   12.1.0
   12.0.0
   11.3.0
```

src/decode.c

```
@@ -186,7 +186,8 @@ _setimage(ImagingDecoderObject *decoder, PyObject *args)
 {
             state->ysize = y1 - y0;
         }
-    if (state->xsize <= 0 || state->xsize + state->xoff > (int)im->xsize ||
+    if (state->xoff < 0 || state->xsize <= 0 ||
+        state->xsize + state->xoff > (int)im->xsize || state->yoff < 0 ||
         state->ysize <= 0 || state->ysize + state->yoff > (int)im->ysize) {
         PyErr_SetString(PyExc_ValueError, "tile cannot extend outside image");
         return NULL;
```

src/encode.c

```
@@ -254,7 +254,8 @@ _setimage(ImagingEncoderObject *encoder, PyObject *args)
 {
             state->ysize = y1 - y0;
         }
```

```
256  256
257       -     if (state->xsize <= 0 || state->xsize + state->xoff > im->xsize ||
          257   +     if (state->xoff < 0 || state->xsize <= 0 ||
          258   +         state->xsize + state->xoff > im->xsize || state->yoff < 0 ||
258  259            state->ysize <= 0 || state->ysize + state->yoff > im->ysize) {
259  260            PyErr_SetString(PyExc_SystemError, "tile cannot extend outside image");
260  261            return NULL;
```

Comments 0

Please sign in to comment.