

authorZdenek Hutyra <zhutyra@centrum.cz>2024-08-30 13:16:39 +0100

committerChris Liddell <chris.liddell@artifex.com>2024-09-18 14:34:34 +0100

commitf49812186baa7d1362880673408a6fbe8719b4f8(patch)

treeaacca4e157e47f74f256327c5b222730d0027d6e

parent85bd9d2f4b792fe67aef22f1a4117457461b8ba6(diff)

diff options

context:3

space:include

mode:unified

PS interpreter - check the type of the Pattern Implementation

Bug #707991

See bug report for details.

CVE-2024-46951

Diffstat

-rw-r--r-- psi/zcolor.c 3

1 files changed, 3 insertions, 0 deletions

diff --git a/psi/zcolor.c b/psi/zcolor.c

index d4e7a4438..d3384d75d 100644

--- a/psi/zcolor.c

+++ b/psi/zcolor.c

@@ -5276,6 +5276,9 @@ static int patterncomponent(i_ctx_t * i_ctx_p, ref *space, int *n)

code = array_get(imemory, pImpl, 0, &pPatInst);

if (code < 0)

return code;

+ if (!r_is_struct(&pPatInst) || (!r_has_stype(&pPatInst, imemory, st_pattern1_instance) && !r_has_stype(&pPatInst, imemory, st_pattern2

+ return_error(gs_error_typecheck);

+ cc.pattern = r_ptr(&pPatInst, gs_pattern_instance_t);

if (pattern_instance_uses_base_space(cc.pattern))

*n = n_comps;