Bug 1970987 (CVE-2021-3598) - CVE-2021-3598 OpenEXR: Heap buffer overflow in Imf_3_1::CharPtrIO::readChars

Keywords:	Security ×
Status:	NEW
Alias:	CVE-2021-3598
Product:	Security Response
Component:	vulnerability
Version:	unspecified
Hardware:	All
OS:	Linux
Priority:	low
Severity:	low
Target Milestone:	---
Assignee:	Red Hat Product Security
QA Contact:	
Docs Contact:	
URL:	
Whiteboard:	
Depends On:	~~1970988~~ ~~1970989~~ 1973408 1973409 2023361
Blocks:	1970995 1971055
TreeView+	depends on / blocked

Reported:	2021-06-11 15:39 UTC by Pedro Sampaio
Modified:	2021-12-21 08:11 UTC (History)
CC List:	5 users (show)
Fixed In Version:	OpenEXR 3.0.5
Doc Type:	If docs needed, set a value
Doc Text:	There's a flaw in OpenEXR's ImfDeepScanLineInputFile functionality. An attacker who is able to submit a crafted file to an application linked with OpenEXR could cause an out-of-bounds read. The greatest risk from this flaw is to application availability.
Clone Of:	
Environment:	
Last Closed:	

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Pedro Sampaio 2021-06-11 15:39:32 UTC Description

A heap-buffer overflow was found in the readChars function of OpenEXR in versions before 3.0.3. An attacker could use this flaw to execute arbitrary code with the permissions of the user running the application compiled against OpenEXR.

Upstream issue:

https://github.com/AcademySoftwareFoundation/openexr/issues/1033

Upstream patch:

https://github.com/AcademySoftwareFoundation/openexr/pull/1037/commits/b0eeb890016a8c9dc0830f0b7be5a9c52cb829d4

Pedro Sampaio 2021-06-11 15:40:04 UTC Comment 1

Created OpenEXR tracking bugs for this issue:

Affects: fedora-all [~~bug 1970988~~]

Created mingw-OpenEXR tracking bugs for this issue:

Affects: fedora-all [~~bug 1970989~~]

Note

You need to log in before you can comment on or make changes to this bug.