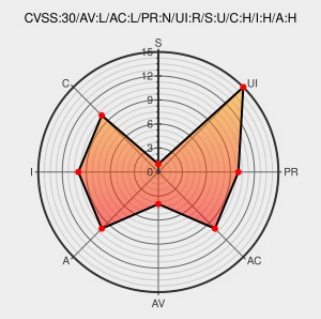
CVE-2017-12596

Published on: 08/06/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:30 PM UTC

CVE-2017-12596

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openexr from Openexr contain the following vulnerability:

In OpenEXR 2.2.0, a crafted image causes a heap-based buffer over-read in the hufDecode function in IlmImf/ImfHuf.cpp during exrmaketiled execution; it may result in denial of service or possibly unspecified other impact.

CVE-2017-12596 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
USN-4148-1: OpenEXR vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4148-1
Release v2.3.0 · AcademySoftwareFoundation/openexr · GitHub	github.com text/html	CONFIRM github.com/openexr/openexr/releases/tag/v2.3.0

[SECURITY] [DLA 2358-1] openexr security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200830 [SECURITY] [DLA 2358-1] openexr security update
pocs/openexr.md at master · xiaoqx/pocs · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/xiaoqx/pocs/blob/master/openexr.md
heap-based buffer overflow in exrmaketiled · Issue #238 · openexr/openexr · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/openexr/openexr/issues/238

Related QID Numbers

502131 Alpine Linux Security Update for openexr

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openexr	Openexr	2.2.0	All	All	All
Application	Openexr	Openexr	2.2.0	All	All	All

cpe:2.3:a:openexr:openexr:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:openexr:openexr:2.2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→