

✓ Out-of-bounds memory access due to malformed DDS image file

Actions

✓ Closed, Resolved

Public

BUG

Assigned To

Sergey Sharybin (sergey)

Authored By

Albin Eldstål-Ahrens (eldstal)

Jan 5 2022, 2:21 PM

Tags

BF Blender (Backlog)

Images & Movies (Backlog)

Subscribers

Albin Eldstål-Ahrens (eldstal)

Evan Wilson (EAW)

Philipp Oeser (lichtwerk)

Sergey Sharybin (sergey)

Description

System Information

Operating system: Windows-10-10.0.19044-SP0 64 Bits

Graphics card: Radeon RX 580 Series ATI Technologies Inc. 4.5.14761 Core Profile Context 21.10.3 30.0.13031.1001

Blender Version

Broken: version: 3.1.0 Alpha, branch: master, commit date: 2021-12-31 20:32, hash: rB6844304dda49

Broken: version: 2.93.8 Release Candidate, branch: master, commit date: 2021-12-15 14:37, hash: rB59a48cc43daf

Worked: -

Short description of error

A DDS image may be smaller than expected, leading to an integer underflow and an out-of-bounds read.

Cause

The size calculation at `source/blender/imbuf/intern/dds/DirectDrawSurface.cpp:1117` assumes that the total stream size is larger than the DDS header (128 Bytes).

A file with an otherwise valid header, but a file size smaller than 128 bytes can reach this point. `uint size` underflows

to `0xffffffff`, which is clearly larger than the buffer.

This large size also bypasses the bounds check in `mem_read()` at `source/blender/imbuf/intern/dds/Stream.cpp:87` due to another integer overflow.

Exact steps for others to reproduce the error

The following input file illustrates the problem.

 **oobr_DirectDrawSurface_1123.dds** 127 B
Download

- 1. Start with the default new project
- 2. Open the material panel.
- 3. Set the material "base color" of the default cube to "Image texture"
- 4. Load the texture file `oobr_DirectDrawSurface_1123.dds`.

After a second or so, Blender crashes.

Impact

An out-of-bounds read can potentially be used to bypass security mechanisms such as stack cookies or pointer encryption.

Proposed mitigation

- 1. Add a bounds check in `DirectDrawSurface::readData()`
- 2. Possibly harden `dds/Stream` against similar overflows by using a wider datatype during comparisons.

Revisions and Commits

rB Blender


rB0ac83d05d7cc [Fix T94661: Out-of-bounds memory access due to malformed DDS image file](#)


rBbbad834f1c2a [Fix T94661: Out-of-bounds memory access due to malformed DDS image file](#)


rBd9dd8c287f57 [Fix T94661: Out-of-bounds memory access due to malformed DDS image file](#)

Related Objects

Mentions	
Mentioned In	
	T77348: Blender LTS: Maintenance Task 2.83
	T88449: Blender LTS: Maintenance Task 2.93
Mentioned Here	
	T86952: Heap Buffer Overflow when viewing dds thumbnails in the file browser.
	T94629: Out of bounds memory access in IMB_flipy() due to large image dimensions
	D11952: Fix T89542: Crash when loading certain .hdr files

 **Albin Eldstål-Ahrens (eldstal)** created this task. Jan 5 2022, 2:21 PM

 **Philipp Oeser (lichtwerk)** changed the task status from *Needs Triage* to *Confirmed*. Jan 5 2022, 2:48 PM

 **Philipp Oeser (lichtwerk)** added a project: **Images & Movies**.

 **Philipp Oeser (lichtwerk)** added subscribers: **Sergey Sharybin (sergey)**, **Philipp Oeser (lichtwerk)**.

Can confirm.

T94629: Out-of-bounds memory access in IMB_flipy() due to large image dimensions /


D11952: Fix T89542: Crash when loading certain .hdr files are related.


CC [@Sergey Sharybin \(sergey\)](#)

 **Evan Wilson (EAW)** added a subscriber: **Evan Wilson (EAW)**. Jan 5 2022, 6:08 PM


T86952: Heap Buffer Overflow when viewing dds thumbnails in the file browser. I would think is also related, as it involves a Heap Buffer overflow in the dds flipping function.

 <https://developer.blender.org/diffusion/B/browse/master/source/blender/imbuf/intern/dds/FlipDXT.cpp>


 **Aaron Carlisle (Blendify)** changed the subtype of this task from "Report" to "Bug". Jan 7 2022, 3:11 AM


 **Sergey Sharybin (sergey)** closed this task as *Resolved* by committing **rBd9dd8c287f57: Fix T94661: Out-of-bounds memory access due to malformed DDS image file**. Jan 10 2022, 2:29 PM

 **Sergey Sharybin (sergey)** claimed this task.

 **Sergey Sharybin (sergey)** added a commit: **rBd9dd8c287f57: Fix T94661: Out-of-bounds memory access due to malformed DDS image file**.

 **Philipp Oeser (lichtwerk)** mentioned this in **T88449: Blender LTS: Maintenance Task 2.93**. Jan 11 2022, 12:41 PM

 **Philipp Oeser (lichtwerk)** added a commit: **rBbbad834f1c2a: Fix T94661: Out-of-bounds memory access due to malformed DDS image file**. Jan 11 2022, 4:00 PM

 **Philipp Oeser (lichtwerk)** added a commit: **rB0ac83d05d7cc: Fix T94661: Out-of-bounds memory access due to malformed DDS image file**. Jan 18 2022, 10:54 AM

 **Philipp Oeser (lichtwerk)** mentioned this in ~~**T77348: Blender LTS: Maintenance Task 2.83**~~. Jan 18 2022, 10:54 AM

 **Albin Eldstål-Ahrens (eldstal)** added a comment. Feb 9 2022, 11:32 AM

This vulnerability has been assigned CVE-2022-0544 by the Red Hat CNA.

[Log In to Comment](#)