



CVE-2005-4470

Published on: 12/21/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4470

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Blenloader](#) from [Blender](#) contain the following vulnerability:

Heap-based buffer overflow in the `get_bhead` function in `readfile.c` in Blender `BlenLoader` 2.0 through 2.40pre allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a `.blend` file with a negative `bhead.len` value, which causes less memory to be allocated than expected, possibly due to an integer overflow.

CVE-2005-4470 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20051220 \[Overflow.pl\] Blender
BlenLoader Integer Overflow](#)

Secunia - Advisories - Blender "get_bhead()" Integer
Overflow Vulnerability

[Vendor Advisory](#)
web.archive.org
text/html

[SECUNIA 18176](#)

USN-238-2: Blender vulnerability | Ubuntu security
notices

usn.ubuntu.com
text/html

[UBUNTU USN-238-2](#)

Secunia - Advisories - Ubuntu update for blender

web.archive.org
text/html

[SECUNIA 18178](#)

404 Not Found

[Exploit](#)

[MISC www.overflow.pl/adv/blenderinteger.txt](#)

www.overflow.pl[text/plain](#)[Inactive Link](#) [Not Archived](#)

Secunia - Advisories - Gentoo update for blender

web.archive.org[text/html](#) SECUNIA 18452

Debian -- Security Information -- DSA-1039-1 blender

www.debian.org[Deprecated Link](#)[text/html](#) DEBIAN DSA-1039

Blender BlenLoader File Processing Integer Overflow Vulnerability

[Exploit](#)[cve.report \(archive\)](#)[text/html](#) BID 15981

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.vupen.com[text/html](#) VUPEN ADV-2005-3032

Secunia - Advisories - Debian update for blender

web.archive.org[text/html](#) SECUNIA 19754

Gentoo Linux Documentation -- Blender: Heap-based buffer overflow

www.gentoo.org[text/html](#) GENTOO GLSA-200601-08

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Blender	Blenloader	2.0	All	All	All
Application	Blender	Blenloader	2.04	All	All	All
Application	Blender	Blenloader	2.25	All	All	All
Application	Blender	Blenloader	2.26	All	All	All
Application	Blender	Blenloader	2.27	All	All	All
Application	Blender	Blenloader	2.28	All	All	All
Application	Blender	Blenloader	2.28a	All	All	All
Application	Blender	Blenloader	2.28c	All	All	All
Application	Blender	Blenloader	2.30	All	All	All
Application	Blender	Blenloader	2.31a	All	All	All
Application	Blender	Blenloader	2.32	All	All	All
Application	Blender	Blenloader	2.33	All	All	All
Application	Blender	Blenloader	2.33a	All	All	All
Application	Blender	Blenloader	2.34	All	All	All
Application	Blender	Blenloader	2.35	All	All	All

Application	Blender	Blenloader	2.37	All	All	All
Application	Blender	Blenloader	2.37a	All	All	All
Application	Blender	Blenloader	2.39	All	All	All
Application	Blender	Blenloader	2.40_alpha	All	All	All
Application	Blender	Blenloader	2.0	All	All	All
Application	Blender	Blenloader	2.04	All	All	All
Application	Blender	Blenloader	2.25	All	All	All
Application	Blender	Blenloader	2.26	All	All	All
Application	Blender	Blenloader	2.27	All	All	All
Application	Blender	Blenloader	2.28	All	All	All
Application	Blender	Blenloader	2.28a	All	All	All
Application	Blender	Blenloader	2.28c	All	All	All
Application	Blender	Blenloader	2.30	All	All	All
Application	Blender	Blenloader	2.31a	All	All	All
Application	Blender	Blenloader	2.32	All	All	All
Application	Blender	Blenloader	2.33	All	All	All
Application	Blender	Blenloader	2.33a	All	All	All
Application	Blender	Blenloader	2.34	All	All	All
Application	Blender	Blenloader	2.35	All	All	All
Application	Blender	Blenloader	2.37	All	All	All
Application	Blender	Blenloader	2.37a	All	All	All
Application	Blender	Blenloader	2.39	All	All	All
Application	Blender	Blenloader	2.40_alpha	All	All	All
Application	Blender	Blenloader	All	All	All	All
cpe:2.3:a:blender:blenloader:2.0:*****:						
cpe:2.3:a:blender:blenloader:2.04:*****:						
cpe:2.3:a:blender:blenloader:2.25:*****:						
cpe:2.3:a:blender:blenloader:2.26:*****:						
cpe:2.3:a:blender:blenloader:2.27:*****:						
cpe:2.3:a:blender:blenloader:2.28:*****:						
cpe:2.3:a:blender:blenloader:2.28a:*****:						
cpe:2.3:a:blender:blenloader:2.28c:*****:						
cpe:2.3:a:blender:blenloader:2.30:*****:						

cpe:2.3:a:blender:blenloader:2.31a:*****:
cpe:2.3:a:blender:blenloader:2.32:*****:
cpe:2.3:a:blender:blenloader:2.33:*****:
cpe:2.3:a:blender:blenloader:2.33a:*****:
cpe:2.3:a:blender:blenloader:2.34:*****:
cpe:2.3:a:blender:blenloader:2.35:*****:
cpe:2.3:a:blender:blenloader:2.37:*****:
cpe:2.3:a:blender:blenloader:2.37a:*****:
cpe:2.3:a:blender:blenloader:2.39:*****:
cpe:2.3:a:blender:blenloader:2.40_alpha:*****:
cpe:2.3:a:blender:blenloader:2.0:*****:
cpe:2.3:a:blender:blenloader:2.04:*****:
cpe:2.3:a:blender:blenloader:2.25:*****:
cpe:2.3:a:blender:blenloader:2.26:*****:
cpe:2.3:a:blender:blenloader:2.27:*****:
cpe:2.3:a:blender:blenloader:2.28:*****:
cpe:2.3:a:blender:blenloader:2.28a:*****:
cpe:2.3:a:blender:blenloader:2.28c:*****:
cpe:2.3:a:blender:blenloader:2.30:*****:
cpe:2.3:a:blender:blenloader:2.31a:*****:
cpe:2.3:a:blender:blenloader:2.32:*****:
cpe:2.3:a:blender:blenloader:2.33:*****:
cpe:2.3:a:blender:blenloader:2.33a:*****:
cpe:2.3:a:blender:blenloader:2.34:*****:
cpe:2.3:a:blender:blenloader:2.35:*****:
cpe:2.3:a:blender:blenloader:2.37:*****:
cpe:2.3:a:blender:blenloader:2.37a:*****:
cpe:2.3:a:blender:blenloader:2.39:*****:
cpe:2.3:a:blender:blenloader:2.40_alpha:*****:

cpe:2.3:a:blender:blenloader:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)