



CVE-2013-1872

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2013-1872
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-19 23:55:00 UTC
Updated	2023-11-07 02:14:00 UTC
Description	The Intel drivers in Mesa 8.0.x and 9.0.x allow context-dependent attackers to cause a denial of service (reachable assertio

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Application	Mesa3d	Mesa	8.0	All	All	All
Application	Mesa3d	Mesa	8.0.1	All	All	All
Application	Mesa3d	Mesa	8.0.2	All	All	All
Application	Mesa3d	Mesa	8.0.3	All	All	All
Application	Mesa3d	Mesa	8.0.4	All	All	All
Application	Mesa3d	Mesa	8.0.5	All	All	All
Application	Mesa3d	Mesa	9.0	All	All	All
Application	Mesa3d	Mesa	9.0.1	All	All	All
Application	Mesa3d	Mesa	9.0.2	All	All	All
Application	Mesa3d	Mesa	9.0.3	All	All	All
Application	Mesa3d	Mesa	8.0	All	All	All

Application	Mesa3d	Mesa	8.0.1	All	All	All
Application	Mesa3d	Mesa	8.0.2	All	All	All
Application	Mesa3d	Mesa	8.0.3	All	All	All
Application	Mesa3d	Mesa	8.0.4	All	All	All
Application	Mesa3d	Mesa	8.0.5	All	All	All
Application	Mesa3d	Mesa	9.0	All	All	All
Application	Mesa3d	Mesa	9.0.1	All	All	All
Application	Mesa3d	Mesa	9.0.2	All	All	All
Application	Mesa3d	Mesa	9.0.3	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

References

Reference	Source	Link
USN-1888-1: Mesa vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Mageia Advisory: MGASA-2013-0190 - Updated mesa packages fix multiple vulnerabilities	CONFIRM	advisories.mageia.org
Mesa Out of Bounds CVE-2013-1872 Memory Corruption Vulnerability	BID	www.bidsa.org
Debian -- Security Information -- DSA-2704-1 mesa	DEBIAN	www.debian.org
Red Hat Customer Portal	MISC	access.redhat.com
[security-announce] SUSE-SU-2013:1175-1: important: Security update for	SUSE	lists.opensuse.org
Red Hat Customer Portal	REDHAT	redhat.com
CVE-2013-1872 - Red Hat Customer Portal	MISC	access.redhat.com
923584 – (CVE-2013-1872) CVE-2013-1872 Mesa: Memory corruption (OOB read/write) on intel drivers	CONFIRM	bugzilla.redhat.com
59429 – brw_fs.cpp:1466: bool fs_visitor::remove_dead_constants(): Assertion `constant_nr < (int)c->prog_data.nr_params	MISC	bugzilla.redhat.com
[security-announce] openSUSE-SU-2013:1188-1: important: Mesa: security f	SUSE	lists.opensuse.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)