



# CVE-2018-10689

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

## Summary

<b>CVE</b>	CVE-2018-10689
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-05-03 07:29:00 UTC
<b>Updated</b>	2023-11-07 02:51:00 UTC
<b>Description</b>	blktrace (aka Block IO Tracing) 1.2.0, as used with the Linux kernel and Android, has a buffer overflow in the dev_map_rea

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Blktrace Project</a>	<a href="#">Blktrace</a>	1.2.0	All	All	All
Application	<a href="#">Blktrace Project</a>	<a href="#">Blktrace</a>	1.2.0	All	All	All
Application	<a href="#">Blktrace Project</a>	<a href="#">Blktrace</a>	1.2.0	All	All	All
Application	<a href="#">Blktrace Project</a>	<a href="#">Blktrace</a>	1.2.0	All	All	All

## References

Reference	Source	Link	Tags
kernel/git/axboe/blktrace.git - blktrace/parse repo	MISC	<a href="#">git.kernel.org</a>	Patch
blktrace: Buffer overflow (GLSA 202107-15) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	
A heap overflow in blktrace — Linux Btrace	MISC	<a href="#">www.spinics.net</a>	Mailing List, Third Party Advisory
git.kernel.dk Git - blktrace.git/log		<a href="#">git.kernel.dk</a>	
Blktrace 'btt/devmap.c' Local Buffer Overflow Vulnerability	BID	<a href="#">www.securityfocus.com</a>	Third Party Advisory, VDB Entry
git.kernel.dk Git - blktrace.git/log	MISC	<a href="#">git.kernel.dk</a>	Issue Tracking, Third Party Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">377522</a> Alibaba Cloud Linux Security Update for blktrace (ALINUX2-SA-2019:0056)
<a href="#">670362</a> EulerOS Security Update for blktrace (EulerOS-SA-2021-1768)
<a href="#">670598</a> EulerOS Security Update for blktrace (EulerOS-SA-2021-2356)
<a href="#">710061</a> Gentoo Linux blktrace Buffer overflow (GLSA 202107-15)
<a href="#">900247</a> CBL-Mariner Linux Security Update for blktrace 1.2.0
<a href="#">901573</a> Common Base Linux Mariner (CBL-Mariner) Security Update for blktrace (6328-1)
<a href="#">903341</a> Common Base Linux Mariner (CBL-Mariner) Security Update for blktrace (1802)

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

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