



CVE-2018-10229

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

Summary

CVE	CVE-2018-10229
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-04 20:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A hardware vulnerability in GPU memory modules allows attackers to accelerate micro-architectural attacks through the use

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	-	All	All	All
Application	Google	Chrome	-	All	All	All
Hardware	Lg	Nexus 5	-	All	All	All
Hardware	Lg	Nexus 5	-	All	All	All
Application	Mozilla	Firefox	-	All	All	All
Application	Mozilla	Firefox	-	All	All	All

References

Reference	Source	Link	Tags
Multiple Devices Integrated GPUs CVE-2018-10229 Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party Adviso
www.vusec.net/wp-content/uploads/2018/05/glitch.pdf	MISC	www.vusec.net	Technical Descrip
CERT Vulnerability Notes Database	CERT-VN	www.kb.cert.org	Third Party Adviso
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

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](#).

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

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