



CVE-2012-0946

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

Summary

CVE	CVE-2012-0946
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-22 18:55:00 UTC
Updated	2017-12-29 02:29:00 UTC
Description	The NVIDIA UNIX driver before 295.40 allows local users to access arbitrary memory locations by leveraging GPU device-r

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nvidia	Unix Driver	All	All	All	All

References

Reference	Source
Security vulnerability CVE-2012-0946 in the NVIDIA UNIX driver	COM
Security Advisory SA48650 - NVIDIA Graphics Drivers for Linux GPU Device Node Access Privilege Escalation Vulnerability - Secunia	SEC
USN-1420-1: NVIDIA graphics drivers vulnerability Ubuntu	UBL
Security Advisory SA48793 - Ubuntu update for nvidia-graphics-drivers - Secunia	SEC
IBM X-Force Exchange	XF
CVE Program record	CVE
NVD vulnerability detail	NVD

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](#)