



CVE-2013-4577

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-4577
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-12 14:55:00 UTC
Updated	2024-01-16 01:15:00 UTC
Description	A certain Debian patch for GNU GRUB uses world-readable permissions for grub.cfg, which allows local users to obtain pas

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Grub	-	All	All	All
Application	Gnu	Grub	-	All	All	All

References

Reference

#632598 - grub-mkconfig: CVE-2013-4577: should set safer permissions even when hashed passwords are found - Debian Bug report logs

oss-sec: CVE Request: grub-mkconfig

oss-sec: Re: CVE Request: grub-mkconfig

oss-security - CVE-2023-4001: a password bypass vulnerability in the downstream GRUB boot manager

CVE Program record

NVD vulnerability detail

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](#)