



CVE-2011-3349

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

Summary

CVE	CVE-2011-3349
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-19 22:15:00 UTC
Updated	2019-12-03 16:19:00 UTC
Description	lightdm before 0.9.6 writes in .dmrc and Xauthority files using root permissions while the files are in user controlled folders.

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lightdm Project	Lightdm	All	All	All	All
Application	Lightdm Project	Lightdm	All	All	All	All

References

Reference	Source	Link	T
LightDM Symlink Attack Local Privilege Escalation Vulnerability	MISC	www.securityfocus.com	TI
Bug #834079 "files written as root to user-controlled folders" : Bugs : lightdm package : Debian	MISC	bugs.launchpad.net	TI
Red Hat Customer Portal	MISC	access.redhat.com	B
#639151 - Local privilege escalation - Debian Bug report logs	MISC	bugs.debian.org	M
oss-sec: lightdm issues	MISC	seclists.org	M
CVE-2011-3349	MISC	security-tracker.debian.org	TI
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

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](#)