



CVE-2011-3602

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

Summary

CVE	CVE-2011-3602
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-27 21:55:00 UTC
Updated	2023-11-07 02:08:00 UTC
Description	Directory traversal vulnerability in device-linux.c in the router advertisement daemon (radvd) before 1.8.2 allows local users

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Litech	Router Advertisement Daemon	All	All	All	All

References

Reference	Source	Link
www.litech.org/radvd/CHANGES	CONFIRM	www.litech.org
oss-security - radvd 1.8.2 released with security fixes	MLIST	www.openwall.com
USN-1257-1: radvd vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Debian -- Security Information -- DSA-2323-1 radvd	DEBIAN	www.debian.org
set_interface_var() doesn't check interface name and blindly does · reubenhwk/radvd@92e22ca · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)