CVE-2011-1549

MITRE NVD CVE.ORG JSON API Print: PDF

Summary

CVE	CVE-2011-1549
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-30 22:55:00 UTC
Updated	2011-04-21 02:33:00 UTC
Description	The default configuration of logrotate on Gentoo Linux uses root privileges to process files in directories that permit non-roo

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Application	Gentoo	Logrotate	All	All	All	All
Application	Gentoo	Logrotate	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	

oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
logrotate Gentoo Linux 'var/log/' Symlink Local Privilege Escalation Vulnerability	BID	www.securityfocus.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - Re: CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
oss-security - CVE Request -- logrotate -- nine issues	MLIST	openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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