



CVE-2012-2093

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

Summary

CVE	CVE-2012-2093
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-18 22:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	src/common/latex.py in Gajim 0.15 allows local users to overwrite arbitrary files via a symlink attack on a temporary latex file

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gajim	Gajim	0.15	All	All	All
Application	Gajim	Gajim	0.15	All	All	All

References

Reference	Source	Link	Tags
Security Advisory SA48794 - Debian update for gajim - Secunia	SECUNIA	secunia.com	
[SECURITY] Fedora 16 Update: gajim-0.15-2.fc16	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 17 Update: gajim-0.15-2.fc17	FEDORA	lists.fedoraproject.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
oss-security - Re: gajim insecure file creation when using latex	MLIST	www.openwall.com	
Sign in · GitLab	CONFIRM	trac.gajim.org	
oss-security - gajim insecure file creation when using latex	MLIST	www.openwall.com	
Gajim CVE-2012-2093 Insecure Temporary File Creation Vulnerability	BID	www.securityfocus.com	
Gentoo Linux Documentation -- Gajim: Multiple vulnerabilities	GENTOO	security.gentoo.org	
[SECURITY] Fedora 15 Update: gajim-0.15-2.fc15	FEDORA	lists.fedoraproject.org	
Authentication portal	CONFIRM	hg.gajim.org	
Security Alerts - Secunia	SECUNIA	secunia.com	Vendor Advisory

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.			

© 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