



CVE-2004-0064

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

Summary

CVE	CVE-2004-0064
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-02-17 05:00:00 UTC
Updated	2016-10-18 02:40:00 UTC
Description	The SuSEconfig.gnome-filesystem script for YaST in SuSE 9.0 allows local users to overwrite arbitrary files via a symlink at

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	All	All

References

Reference	Source
'SuSE linux 9.0 YaST config Skript [exploit]' - MARC	BUGT
SuSE YaST SuSEconfig.gnome-filesystem Local Insecure File Creation Symlink Vulnerability	BID
SuSEconfig.gnome-filesystem Temporary File Symlink Flaw Lets Local Users Overwrite Files With Root Privileges - SecurityTracker	SECTI
3460	OSVD
Secunia - Advisories - SuSE "SuSEconfig.gnome-filesystem" Insecure Temporary File Creation	SECU
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#)