



CVE-2010-0230

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

Summary

CVE	CVE-2010-0230
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-01-22 21:30:00 UTC
Updated	2011-04-28 04:00:00 UTC
Description	SUSE Linux Enterprise 10 SP3 (SLE10-SP3) and openSUSE 11.2 configures postfix to listen on all network interfaces, whi

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Suse	Opensuse	11.2	All	All	All
Operating System	Suse	Opensuse	11.2	All	All	All
Operating System	Suse	Suse Linux	10	sp3	enterprise_desktop	All
Operating System	Suse	Suse Linux	10	sp3	enterprise_server	All
Operating System	Suse	Suse Linux	10	sp3	enterprise_desktop	All
Operating System	Suse	Suse Linux	10	sp3	enterprise_server	All

References

Reference	Source	Link	Tags
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:001	SUSE	lists.opensuse.org	Vendor Advisory
[security-announce] SUSE Security Announcement: postfix (SUSE-SA:2010:01	SUSE	lists.opensuse.org	
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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)