



CVE-2012-2337

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2012-2337
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-18 18:55:00 UTC
Updated	2018-01-05 02:29:00 UTC
Description	sudo 1.6.x and 1.7.x before 1.7.9p1, and 1.8.x before 1.8.4p5, does not properly support configurations that use a netmask

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Todd Miller	Sudo	1.6	All	All	All
Application	Todd Miller	Sudo	1.6.1	All	All	All
Application	Todd Miller	Sudo	1.6.2	All	All	All
Application	Todd Miller	Sudo	1.6.2p3	All	All	All
Application	Todd Miller	Sudo	1.6.3	All	All	All
Application	Todd Miller	Sudo	1.6.3_p7	All	All	All
Application	Todd Miller	Sudo	1.6.4	All	All	All
Application	Todd Miller	Sudo	1.6.4p2	All	All	All
Application	Todd Miller	Sudo	1.6.5	All	All	All
Application	Todd Miller	Sudo	1.6.6	All	All	All
Application	Todd Miller	Sudo	1.6.7	All	All	All
Application	Todd Miller	Sudo	1.6.7p5	All	All	All
Application	Todd Miller	Sudo	1.6.8	All	All	All
Application	Todd Miller	Sudo	1.6.8p12	All	All	All
Application	Todd Miller	Sudo	1.6.9	All	All	All
Application	Todd Miller	Sudo	1.6.9p20	All	All	All
Application	Todd Miller	Sudo	1.6.9p21	All	All	All

Application	Todd Miller	Sudo	1.6.9p22	All	All	All
Application	Todd Miller	Sudo	1.6.9p23	All	All	All
Application	Todd Miller	Sudo	1.6	All	All	All
Application	Todd Miller	Sudo	1.6.1	All	All	All
Application	Todd Miller	Sudo	1.6.2	All	All	All
Application	Todd Miller	Sudo	1.6.2p3	All	All	All
Application	Todd Miller	Sudo	1.6.3	All	All	All
Application	Todd Miller	Sudo	1.6.3_p7	All	All	All
Application	Todd Miller	Sudo	1.6.4	All	All	All
Application	Todd Miller	Sudo	1.6.4p2	All	All	All
Application	Todd Miller	Sudo	1.6.5	All	All	All
Application	Todd Miller	Sudo	1.6.6	All	All	All
Application	Todd Miller	Sudo	1.6.7	All	All	All
Application	Todd Miller	Sudo	1.6.7p5	All	All	All
Application	Todd Miller	Sudo	1.6.8	All	All	All
Application	Todd Miller	Sudo	1.6.8p12	All	All	All
Application	Todd Miller	Sudo	1.6.9	All	All	All
Application	Todd Miller	Sudo	1.6.9p20	All	All	All
Application	Todd Miller	Sudo	1.6.9p21	All	All	All
Application	Todd Miller	Sudo	1.6.9p22	All	All	All
Application	Todd Miller	Sudo	1.6.9p23	All	All	All

References

Reference	S
Support / Security / Advisories // MDVSA-2012:079 Mandriva	M
IP addresses in sudoers with netmask may match additional hosts	C
Security Alerts - Secunia	S
CVE-2012-2337 SUSE	M
Bug 820677 – CVE-2012-2337 sudo: Multiple netmask values used in Host / Host_List configuration cause any host to be allowed access	C
Security Alerts - Secunia	S
Debian -- Security Information -- DSA-2478-1 sudo	D
Sudo Netmask Error Lets Remote Authenticated Users Bypass Host Access Controls - SecurityTracker	S
[SECURITY] Fedora 17 Update: sudo-1.8.3p1-7.fc17	F
Security Advisory SA49948 - Red Hat update for sudo - Secunia	S
Security Alerts - Secunia	S

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](#)