



CVE-2015-0272

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

Summary

CVE	CVE-2015-0272
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-17 15:59:00 UTC
Updated	2023-02-13 00:46:00 UTC
Description	GNOME NetworkManager allows remote attackers to cause a denial of service (IPv6 traffic disruption) via a crafted MTU v

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Application	Gnome	Networkmanager	All	All	All	All
Application	Gnome	Networkmanager	-	All	All	All
Application	Gnome	Networkmanager	-	All	All	All
Operating System	Oracle	Linux	7	-	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp2	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp3	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All

Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	All	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	sp1	All	All

References

Reference

[security-announce] SUSE-SU-2015:2350-1: important: Security update for

[security-announce] SUSE-SU-2016:0354-1: important: Security update for

access.redhat.com | CVE-2015-0272

Red Hat Customer Portal

[security-announce] SUSE-SU-2015:2108-1: important: Security update for

[security-announce] SUSE-SU-2016:2074-1: important: Security update for

[security-announce] SUSE-SU-2015:2194-1: important: Security update for

[security-announce] SUSE-SU-2015:2339-1: important: Security update for

Oracle Linux Bulletin - October 2015

GNOME NetworkManager 'ipv6/addrconf.c' Denial of Service Vulnerability

USN-2792-1: Linux kernel vulnerabilities | Ubuntu

[security-announce] SUSE-SU-2015:2292-1: important: Security update for

NetworkManager/NetworkManager - Network connection manager and user applications (mirrored from <https://gitlab.freedesktop.org/NetworkManager>)

Bug 1192132 – CVE-2015-0272 kernel/NetworkManager: remote DoS using IPv6 RA with bogus MTU

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#)