



CVE-2016-3698

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-3698
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-13 19:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	libndp before 1.6, as used in NetworkManager, does not properly validate the origin of Neighbor Discovery Protocol (NDP)

Risk And Classification

Primary CVSS: v3.0 8.1 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-284 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Libndp	Libndp	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
-----------	--------

Debian -- Security Information -- DSA-3581-1 libndp	af854a3a-2
oss-security - RHSA-2016:1086 libndp: denial of service due to insufficient validation of source of NDP messages	af854a3a-2
Red Hat Customer Portal	af854a3a-2
libndb: reject redirect and router advertisements from non-link-local · jpirko/libndp@2af9a55 · GitHub	af854a3a-2
Oracle Linux Bulletin - April 2016	af854a3a-2
USN-2980-1: libndp vulnerability Ubuntu	af854a3a-2
libndp: validate the IPv6 hop limit · jpirko/libndp@a4892df · GitHub	af854a3a-2
Red Hat Customer Portal	MITRE
CVE-2016-3698 - Red Hat Customer Portal	MITRE
1329366 – (CVE-2016-3698) CVE-2016-3698 libndp: denial of service due to insufficient validation of source of NDP messages	MITRE
CVE Program record	CVE.ORG
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](#)