



# Ovn: ovn: information disclosure via crafted dhcpv6 packets

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

## Summary

<b>CVE</b>	CVE-2026-5367
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 13:16:21 UTC
<b>Updated</b>	2026-04-29 18:16:04 UTC

**Description** A flaw was found in OVN (Open Virtual Network). A remote attacker, by sending crafted DHCPv6 (Dynamic Host Configura

## Risk And Classification

**Primary CVSS:** v3.1 8.6 HIGH from secalert@redhat.com

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

**EPSS:** 0.000600000 probability, percentile 0.183200000 (date 2026-05-05)

**Problem Types:** CWE-130 | CWE-130 Improper Handling of Length Parameter Inconsistency

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Fast Datapath For Red Hat Enterprise Linux 8	unaffected 0:21.12.0-145.el8fdp * rpm	Not specified
CNA	Red Hat	Fast Datapath For Red Hat Enterprise Linux 8	unaffected 0:23.06.4-30.el8fdp * rpm	Not specified
CNA	Red Hat	Fast Datapath For Red Hat Enterprise Linux 9	unaffected 0:23.06.4-30.el9fdp * rpm	Not specified
CNA	Red Hat	Fast Datapath For Red Hat Enterprise Linux 9	unaffected 0:23.09.6-16.el9fdp * rpm	Not specified
CNA	Red Hat	Fast Datapath For Red Hat Enterprise Linux 9	unaffected 0:24.03.7-82.el9fdp * rpm	Not specified
CNA	Red Hat	Fast Datapath For Red Hat Enterprise Linux 9	unaffected 0:25.03.2-100.el9fdp * rpm	Not specified
CNA	Red Hat	Fast Datapath For Red Hat Enterprise Linux 9	unaffected 0:25.09.2-103.el9fdp * rpm	Not specified
CNA	Red Hat	Fast Datapath For RHEL 10	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 10	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 8	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 8	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 8	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 8	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 8	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 9	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

### References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:11695	secalert@redhat.com	<a href="https://access.redhat.com/errata/RHSA-2026:11695">access.redhat.com</a>	
www.openwall.com/lists/oss-security/2026/04/20/3	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.openwall.com/lists/oss-security/2026/04/20/3">www.openwall.com</a>	

access.redhat.com/errata/RHSA-2026:11702	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:11694	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:11698	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:11700	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2026/04/20/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
access.redhat.com/errata/RHSA-2026:11696	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:11701	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-5367	secalert@redhat.com	access.redhat.com	
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.

#### Additional Advisory Data

Source	Time	Event
CNA	2026-04-07T08:10:53.507Z	Reported to Red Hat.
CNA	2026-04-13T00:00:00.000Z	Made public.

#### Workarounds

**CNA:** The only potential mitigation is to disable the DHCPv6 feature for workloads attached to OVN logical ports, e.g.: `ovn-nbctl clear logical_switch_port <workload-port> dhcpv6_options`. We do not recommend mitigating the vulnerability this way because it will also disable legitimate DHCPv6 traffic originating from workloads connected to logical switch ports.

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](#)