Bug 2455863 (CVE-2026-5367) - CVE-2026-5367 ovn: OVN: Information disclosure via crafted DHCPv6 packets

Keywords: Security

Status: NEW

Alias: CVE-2026-5367

Deadline: 2026-04-13

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-04-07 08:12 UTC by OSIDB Bzimport

Modified: 2026-04-24 12:10 UTC (History)

CC List: 5 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-07 08:12:27 UTC Description

```
Multiple versions of OVN (Open Virtual Network) are vulnerable
to
crafted DHCPv6 packets that could potentially read out-of-
bounds,
leaking adjacent info stored on the heap.

OVN supports configuring DHCPv6 options for Logical Switch
Ports.
When configured we allow handling of DHCPv6 requests in a
userspace
thread called pinctrl. The thread accesses user-controlled
packet data
```

and copies some of it in the process of creating a reply
packet.

When building a DHCPv6 ADVERTISE reply, the handler echoes the
Client ID option using the option's self-declared length
without
validating it against the actual packet bounds. A workload can
send
a crafted DHCPv6 SOLICIT with an inflated Client ID length
field,
causing ovn-controller to copy heap memory beyond the valid
packet
data into the reply. The reply is then delivered back to the
attacker's VM port.

Note

You need to log in before you can comment on or make changes to this bug.