Ovn: ovn: heap over-read in icmp error response generation - security issue

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

Summary

CVE	CVE-2026-5265
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 13:16:21 UTC
Updated	2026-04-29 19:16:24 UTC
Description	When generating an ICMP Destination Unreachable or Packet Too Big response, the handler copies a portion of the origina

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from secalert@redhat.com

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

EPSS: 0.000910000 probability, percentile 0.253220000 (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	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

High

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

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 7	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 7	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 7	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 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	Fast Datapath For RHEL 9	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	Fast Datapath For RHEL 9	Not specified	Not specified
CNA	Red Hat	Fast Datapath For RHEL 9	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:11695	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:11702	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2026/04/20/2	af854a3a-2127-422b-91ae-364da2661108	www.openwall.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	
access.redhat.com/errata/RHSA-2026:11696	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2026/04/20/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
access.redhat.com/errata/RHSA-2026:11701	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2026-5265	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.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	2026-03-24T00:00:00.000Z	Reported to Red Hat.
CNA	2026-04-06T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

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