Openvswitch: open vswitch: denial of service via malformed ftp epasv command

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

Summary

CVE	CVE-2026-34956
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-05 16:16:11 UTC
Updated	2026-05-05 19:31:10 UTC
Description	A flaw was found in Open vSwitch. When Open vSwitch is configured with a conntrack flow using FTP helpers over the use

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from secalert@redhat.com

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

Problem Types: CWE-120 | CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
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 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 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 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
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 Enterprise Linux 7	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 OpenStack Platform 13 Queens	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 13 Queens	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 13 Queens	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 16.2	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 16.2	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 17.1	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 17.1	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 18.0	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-34956	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2026/03/31/15	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Seiji Sakurai for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-31T00:00:00.000Z	Reported to Red Hat.
CNA	2026-03-31T00:00:00.000Z	Made public.

Workarounds

CNA: Optionally, avoid using alg=ftp flows. These are not usually configured.

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