



CVE-2016-10377

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

Summary

CVE	CVE-2016-10377
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-29 04:29:00 UTC
Updated	2017-06-08 00:48:00 UTC
Description	In Open vSwitch (OvS) 2.5.0, a malformed IP packet can cause the switch to read past the end of the packet buffer due to a

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openvswitch	Openvswitch	2.5.0	All	All	All
Application	Openvswitch	Openvswitch	2.5.0	All	All	All

References

Reference	Source	Link	Tags
[ovs-dev] [PATCH] flow: Verify that tot_len >= ip_len in miniflow_extract().	CONFIRM	mail.openvswitch.org	Mailing List, Patch, Vendor A
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.

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

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)