



CVE-2021-36980

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

Summary

CVE	CVE-2021-36980
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-20 07:15:00 UTC
Updated	2023-11-26 11:15:00 UTC
Description	Open vSwitch (aka openvswitch) 2.11.0 through 2.15.0 has a use-after-free in decode_NXAST_RAW_ENCAP (called from

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
ofp-actions: Fix use-after-free while decoding RAW_ENCAP. · openvswitch/ovs@6d67310 · GitHub	MISC	github.com	
ofp-actions: Fix use-after-free while decoding RAW_ENCAP. · openvswitch/ovs@9926637 · GitHub	MISC	github.com	
ofp-actions: Fix use-after-free while decoding RAW_ENCAP. · openvswitch/ovs@77cccc7 · GitHub	MISC	github.com	
ofp-actions: Fix use-after-free while decoding RAW_ENCAP. · openvswitch/ovs@38744b1 · GitHub	MISC	github.com	
27851 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	
oss-fuzz-vulns/OSV-2020-2197.yaml at main · google/oss-fuzz-vulns · GitHub	MISC	github.com	
Open vSwitch: Multiple Vulnerabilities (GLSA 202311-16) — Gentoo security		security.gentoo.org	
ofp-actions: Fix use-after-free while decoding RAW_ENCAP. · openvswitch/ovs@65c61b0 · GitHub	MISC	github.com	
ofp-actions: Fix use-after-free while decoding RAW_ENCAP. · openvswitch/ovs@8ce8dc3 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180510	Debian Security Update for openvswitch (CVE-2021-36980)
198488	Ubuntu Security Notification for Open vSwitch Vulnerability (USN-5065-1)
239697	Red Hat Update for OpenShift Container Platform 4.9.0 packages and (RHSA-2021:3758)
501894	Alpine Linux Security Update for openvswitch
710800	Gentoo Linux Open vSwitch Multiple Vulnerabilities (GLSA 202311-16)
752553	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2022:3098-1)
753128	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2022:3099-1)
753244	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2022:3116-1)
754067	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2023:2360-1)
770083	Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2021:3758)
770107	Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2021-3758)
900241	CBL-Mariner Linux Security Update for openvswitch 2.12.3
900946	Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (6781-1)
903536	Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (4611)

© [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](#).

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