



# CVE-2021-3905

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

## Summary

<b>CVE</b>	CVE-2021-3905
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-23 16:15:00 UTC
<b>Updated</b>	2023-11-26 11:15:00 UTC
<b>Description</b>	A memory leak was found in Open vSwitch (OVS) during userspace IP fragmentation processing. An attacker could use this

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	21.10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Openvswitch</a>	<a href="#">Openvswitch</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Fast Datapath</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Fast Datapath</a>	8.0	All	All	All

## References

### Reference

- [Red Hat Customer Portal - Access to 24x7 support and knowledge](#)
- [CVE-2021-3905 | Ubuntu](#)
- [ipf memleak · Issue #226 · openvswitch/ovs-issues · GitHub](#)
- [Open vSwitch: Multiple Vulnerabilities \(GLSA 202311-16\) — Gentoo security](#)
- [2019692 – \(CVE-2021-3905\) CVE-2021-3905 openvswitch: External triggered memory leak in Open vSwitch while processing fragmented packets](#)
- [ipf: release unhandled packets from the batch · openvswitch/ovs@803ed12 · GitHub](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[198640](#) Ubuntu Security Notification for Open vSwitch Vulnerability (USN-5242-1)

[710800](#) Gentoo Linux Open vSwitch Multiple Vulnerabilities (GLSA 202311-16)

[903744](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (10646) (DEPRECATED)

[904008](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (10646-1)

[906109](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (10646-2)

© [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](#)