



CVE-2020-35498

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

Summary

CVE	CVE-2020-35498
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-11 18:15:00 UTC
Updated	2023-11-26 11:15:00 UTC
Description	A vulnerability was found in openvswitch. A limitation in the implementation of userspace packet parsing can allow a malicious

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Openvswitch	Openvswitch	All	All	All	All
Application	Openvswitch	Openvswitch	All	All	All	All

References

Reference	Source
1908845 – (CVE-2020-35498) CVE-2020-35498 openvswitch: limitation in the OVS packet parsing in userspace leads to DoS	MISC
Debian -- Security Information -- DSA-4852-1 openvswitch	DEBIAN
[SECURITY] [DLA 2571-1] openvswitch security update	MLIST
Open vSwitch: Multiple Vulnerabilities (GLSA 202311-16) — Gentoo security	
[SECURITY] Fedora 33 Update: dpdk-20.11-1.fc33 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: dpdk-20.11-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
oss-security - CVE-2020-35498: Open vSwitch: Packet parsing vulnerability	MISC

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[174615](#) SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2021:0439-1)

[239427](#) Red Hat Update for Red Hat OpenStack Platform 13.0 (RHSA-2021:2456)

[281603](#) Fedora Security Update for dpdk (FEDORA-2021-fba11d37ee)

[375504](#) Citrix XenServer Security Updates(CTX306565)

[501656](#) Alpine Linux Security Update for openvswitch

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

[750361](#) OpenSUSE Security Update for openvswitch (openSUSE-SU-2021:0283-1)

[752618](#) SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2022:3384-1)

[900146](#) CBL-Mariner Linux Security Update for openvswitch 2.12.0

[902813](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (3883)

© [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](#)