CVE-2021-3905

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3905
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 16:15:00 UTC
Updated	2023-11-26 11:15:00 UTC
Description	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	Canonical	Ubuntu Linux	21.10	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Openvswitch	Openvswitch	All	All	All	All
Application	Redhat	Enterprise Linux Fast Datapath	7.0	All	All	All
Application	Redhat	Enterprise Linux Fast Datapath	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 pac
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)