



# CVE-2020-8037

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

## Summary

<b>CVE</b>	CVE-2020-8037
<b>State</b>	PUBLIC
<b>Assigner</b>	security@tcpdump.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-04 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	The ppp decapsulator in tcpdump 4.9.3 can be convinced to allocate a large amount of memory.

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	-	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2019-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2019-002	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-002	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-003	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-004	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-005	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-006	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-007	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2021-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	-	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2020-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	supplemental_update	All	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Tcpdump</a>	<a href="#">Tcpdump</a>	4.9.3	All	All	All
Application	<a href="#">Tcpdump</a>	<a href="#">Tcpdump</a>	4.9.3	All	All	All

## References

Reference	Source	Link
PPP: When un-escaping, don't allocate a too-large buffer. · the-tcpdump-group/tcpdump@32027e1 · GitHub	MISC	<a href="#">github.com</a>
[SECURITY] Fedora 33 Update: tcpdump-4.9.3-5.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraprojec</a>
[SECURITY] Fedora 32 Update: tcpdump-4.9.3-4.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraprojec</a>
[SECURITY] Fedora 32 Update: tcpdump-4.9.3-4.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraprojec</a>
Full Disclosure: APPLE-SA-2021-04-26-3 Security Update 2021-002 Catalina	FULLDISC	<a href="#">seclists.org</a>
About the security content of Security Update 2021-002 Catalina - Apple Support	CONFIRM	<a href="#">support.apple.co</a>
About the security content of Security Update 2021-003 Mojave - Apple Support	CONFIRM	<a href="#">support.apple.co</a>
[SECURITY] Fedora 33 Update: tcpdump-4.9.3-5.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraprojec</a>
[SECURITY] [DLA 2444-1] tcpdump security update	MLIST	<a href="#">lists.debian.org</a>
About the security content of macOS Big Sur 11.3 - Apple Support	CONFIRM	<a href="#">support.apple.co</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Hardik Shah

## Legacy QID Mappings

<a href="#">159476</a> Oracle Enterprise Linux Security Update for tcpdump (ELSA-2021-4236)
<a href="#">198735</a> Ubuntu Security Notification for tcpdump Vulnerabilities (USN-5331-2)
<a href="#">239848</a> Red Hat Update for tcpdump (RHSA-2021:4236)
<a href="#">375503</a> Apple macOS Big Sur 11.3 Not Installed (HT212325)
<a href="#">375507</a> Apple macOS Security Update 2021-002 Catalina (HT212326)
<a href="#">375510</a> Apple macOS Security Update 2021-003 Mojave (HT212327)
<a href="#">500687</a> Alpine Linux Security Update for tcpdump

504456 Alpine Linux Security Update for tcpdump
670209 EulerOS Security Update for tcpdump (EulerOS-SA-2021-1708)
670904 EulerOS Security Update for tcpdump (EulerOS-SA-2020-2535)
750583 OpenSUSE Security Update for tcpdump (openSUSE-SU-2020:1986-1)
750584 OpenSUSE Security Update for tcpdump (openSUSE-SU-2020:1983-1)
900152 CBL-Mariner Linux Security Update for tcpdump 4.9.3
901569 Common Base Linux Mariner (CBL-Mariner) Security Update for tcpdump (6905-1)
903121 Common Base Linux Mariner (CBL-Mariner) Security Update for tcpdump (3589)
940158 AlmaLinux Security Update for tcpdump (ALSA-2021:4236)
960756 Rocky Linux Security Update for tcpdump (RLSA-2021:4236)

© [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](#)**