# CVE-2020-8037

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-8037 |
| **State** | PUBLIC |
| **Assigner** | security@tcpdump.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-11-04 18:15:00 UTC |
| **Updated** | 2023-11-07 03:26:00 UTC |
| **Description** | 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 | Apple | Macos | All | All | All | All |
| Operating System | Apple | Mac Os X | All | All | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | - | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2019-001 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2019-002 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2020-001 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2020-002 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2020-003 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2020-004 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2020-005 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2020-006 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2020-007 | All | All |
| Operating System | Apple | Mac Os X | 10.14.6 | security_update_2021-001 | All | All |
| Operating System | Apple | Mac Os X | 10.15.7 | - | All | All |
| Operating System | Apple | Mac Os X | 10.15.7 | security_update_2020-001 | All | All |
| Operating System | Apple | Mac Os X | 10.15.7 | security_update_2021-001 | All | All |
| Operating System | Apple | Mac Os X | 10.15.7 | supplemental_update | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Application | Tcpdump | Tcpdump | 4.9.3 | All | All | All |
| Application | Tcpdump | Tcpdump | 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 | github.com |
| [SECURITY] Fedora 33 Update: tcpdump-4.9.3-5.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraprojec |
| [SECURITY] Fedora 32 Update: tcpdump-4.9.3-4.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraprojec |
| [SECURITY] Fedora 32 Update: tcpdump-4.9.3-4.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraprojec |
| Full Disclosure: APPLE-SA-2021-04-26-3 Security Update 2021-002 Catalina | FULLDISC | seclists.org |
| About the security content of Security Update 2021-002 Catalina - Apple Support | CONFIRM | support.apple.cor |
| About the security content of Security Update 2021-003 Mojave - Apple Support | CONFIRM | support.apple.cor |
| [SECURITY] Fedora 33 Update: tcpdump-4.9.3-5.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraprojec |
| [SECURITY] [DLA 2444-1] tcpdump security update | MLIST | lists.debian.org |
| About the security content of macOS Big Sur 11.3 - Apple Support | CONFIRM | support.apple.cor |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Hardik Shah

## Legacy QID Mappings

159476 Oracle Enterprise Linux Security Update for tcpdump (ELSA-2021-4236)

198735 Ubuntu Security Notification for tcpdump Vulnerabilities (USN-5331-2)

239848 Red Hat Update for tcpdump (RHSA-2021:4236)

375503 Apple MacOS Big Sur 11.3 Not Installed (HT212325)

375507 Apple macOS Security Update 2021-002 Catalina (HT212326)

375510 Apple macOS Security Update 2021-003 Mojave (HT212327)

500687 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)