



CVE-2020-8597

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

Summary

| | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2020-8597 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-02-03 23:15:00 UTC |
| Updated | 2023-11-07 03:26:00 UTC |
| Description | eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions. |

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------------------------|-----------------------------------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Point-to-point Protocol Project | Point-to-point Protocol | All | All | All | All |
| Hardware | Wago | Pfc100 | - | All | All | All |
| Hardware | Wago | Pfc200 | - | All | All | All |
| Operating System | Wago | Pfc Firmware | All | All | All | All |

References

Reference

[pppd 2.4.8 Buffer Overflow ≈ Packet Storm](#)

[Red Hat Customer Portal](#)

[pppd 2.4.8 Buffer Overflow ≈ Packet Storm](#)

pppd: Fix bounds check in EAP code · paulusmack/ppp@8d7970b · GitHub

Debian -- Security Information -- DSA-4632-1 ppp

USN-4288-1: ppp vulnerability | Ubuntu security notices | Ubuntu

Red Hat Customer Portal

VU#782301 - pppd vulnerable to buffer overflow due to a flaw in EAP packet processing

Red Hat Customer Portal

PPP: Buffer overflow (GLSA 202003-19) — Gentoo security

[SECURITY] Fedora 31 Update: ppp-2.4.7-34.fc31 - package-announce - Fedora Mailing-Lists

USN-4288-2: ppp vulnerability | Ubuntu security notices | Ubuntu

Siemens SCALANCE, RUGGEDCOM | CISA

[SECURITY] Fedora 31 Update: ppp-2.4.7-34.fc31 - package-announce - Fedora Mailing-Lists

Security Advisory for Unauthenticated Remote Buffer Overflow Attack in PPPD on WAC510, PSV-2020-0136 | Answer | NETGEAR Support

[security-announce] openSUSE-SU-2020:0286-1: important: Security update

cert-portal.siemens.com/productcert/pdf/ssa-809841.pdf

[SECURITY] Fedora 30 Update: ppp-2.4.7-34.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 30 Update: ppp-2.4.7-34.fc30 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

CVE-2020-8597 PPP Vulnerability in NetApp Products | NetApp Product Security

[SECURITY] [DLA 2097-1] ppp security update

Synology Inc.

Full Disclosure: Buffer overflow in pppd - CVE-2020-8597

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 377087 Alibaba Cloud Linux Security Update for ppp (ALINUX2-SA-2020:0028)
- 377135 Alibaba Cloud Linux Security Update for ppp (ALINUX3-SA-2022:0071)
- 500547 Alpine Linux Security Update for ppp
- 504316 Alpine Linux Security Update for ppp
- 590959 Schneider Electric Easergy T300 Vulnerability (SEVD-2022-011-02)
- 940281 AlmaLinux Security Update for ppp (ALSA-2020:0633)
- 960688 Rocky Linux Security Update for ppp (RLSA-2020:0633)

© [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](#)