CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

### Security Advisory 2020-013

# Critical PPP Daemon Vulnerability

*March 06, 2020 — v1.0*

**TLP:WHITE**

*History:*

- *06/03/2020 — v1.0 – Initial publication*

## Summary

A new dangerous (and 17 years old!) remote code execution vulnerability has been discovered by Ilja Van Sprundel from IOActive [1, 2, 3]. It affects the PPP daemon (`pppd`) software that comes installed on almost all Linux-based operating systems and powers the firmware of many other networking devices. The affected `pppd` software is an implementation of Point-to-Point Protocol (PPP) that enables communication and data transfer between nodes, primarily used to establish Internet links such as those over dial-up modems, DSL broadband connections, and Virtual Private Networks.

The vulnerability is tracked as CVE-2020-8597 with **CVSS Score 9.8** and can be exploited by unauthenticated attackers to remotely execute arbitrary code on affected systems and take full control over them.

## Technical Details

The critical issue is a *stack buffer overflow* vulnerability that exists due to a logical error in the Extensible Authentication Protocol (EAP) packet parser of the `pppd` software, an extension that provides support for additional authentication methods in PPP connections.

For this, all an attacker needs to do is to send an unsolicited malformed EAP packet to a vulnerable ppp client or a server over a direct serial link, ISDN, Ethernet, SSH, socket CAT, PPTP, GPRS, or ATM networks.

Additionally, since `pppd` often runs with high privileges and works in conjunction with kernel drivers, the flaw could allow attackers to potentially execute malicious code with the system or root-level privileges.

This vulnerability is due to an error in validating the size of the input before copying the supplied data into memory. As the validation of the data size is incorrect, arbitrary data can be copied into memory and cause memory corruption, possibly leading to the execution of unwanted code.

The vulnerability is in the logic of the EAP parsing code, specifically in the `eap_request()` and `eap_response()` functions in `eap.c` that are called by a network input handler.

## Products Affected

`pppd` versions 2.4.2 through 2.4.8 —- i.e, all versions released in the last 17 years —- are vulnerable to this new remote code execution vulnerability [1].

Some of the widely-used, popular Linux and BSD distributions listed below have already been confirmed impacted, and many other projects are most likely affected as well:

- Debian
- Ubuntu
- SUSE Linux
- Fedora
- NetBSD
- Red Hat Enterprise Linux

Besides this, the list of other vulnerable applications and devices (some of them listed below) that ship the `pppd` software is also likely extensive, opening a large attack surface for hackers. Examples include [2]:

- Cisco CallManager
- TP-LINK products
- OpenWRT Embedded OS
- Synology products

## Recommendations

Users with affected operating systems and devices are advised to apply security patches as soon as possible, or when they becomes available. Some statements regarding available or planned patches are available in [1]. The updated, non-vulnerable source code is already available in Github [4].

At the time of writing, we are not aware of any public proof-of-concept exploit code for this vulnerability or any in-the-wild exploitation attempts.

## References

[1] https://www.kb.cert.org/vuls/id/782301/

[2] https://thehackernews.com/2020/03/ppp-daemon-vulnerability.html

[3] https://sensorstechforum.com/cve-2020-8597-ppp-daemon-flaw-linux/

[4] https://github.com/paulusmack/ppp