



# CVE-2019-11555

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

## Summary

<b>CVE</b>	CVE-2019-11555
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-26 22:29:00 UTC
<b>Updated</b>	2023-11-07 03:03:00 UTC
<b>Description</b>	The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not valid

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	All	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	All	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	All	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 30 Update: hostapd-2.8-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject</a>
[SECURITY] Fedora 30 Update: wpa_supplicant-2.8-2.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject</a>
USN-3969-2: wpa_supplicant and hostapd vulnerability   Ubuntu security notices	UBUNTU	<a href="#">usn.ubuntu.com</a>
USN-3969-1: wpa_supplicant and hostapd vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>
Index of /security/2019-5	MISC	<a href="#">w1.fi</a>
hostapd and wpa_supplicant: Denial of Service (GLSA 201908-25) — Gentoo security	GENTOO	<a href="#">security.gentoo.o</a>
[SECURITY] [DLA 1867-1] wpa security update	MLIST	<a href="#">lists.debian.org</a>
[SECURITY] Fedora 29 Update: hostapd-2.8-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject</a>
[SECURITY] Fedora 29 Update: hostapd-2.8-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject</a>
[SECURITY] Fedora 30 Update: wpa_supplicant-2.8-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject</a>

oss-security - Re: wpa_supplicant/hostapd: EAP-pwd message reassembly issue with unexpected fragment	MLIST	<a href="http://www.openwall.com">www.openwall.co</a>
w1.fi/security/2019-5/eap-pwd-message-reassembly-issue-with-unexpec...	MISC	<a href="http://w1.fi">w1.fi</a>
oss-security - wpa_supplicant/hostapd: EAP-pwd message reassembly issue with unexpected fragment	MISC	<a href="http://www.openwall.com">www.openwall.co</a>
[SECURITY] Fedora 30 Update: hostapd-2.8-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject">lists.fedoraproject</a>
Bugtraq: [SECURITY] [DSA 4450-1] wpa security update	BUGTRAQ	<a href="http://seclists.org">seclists.org</a>
Debian -- Security Information -- DSA-4450-1 wpa	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Bugtraq: FreeBSD Security Advisory FreeBSD-SA-19:03.wpa	BUGTRAQ	<a href="http://seclists.org">seclists.org</a>
FreeBSD-SA-19:03	FREEBSD	<a href="http://security.FreeBSD">security.FreeBSD</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [500247](#) Alpine Linux Security Update for hostapd
- [500742](#) Alpine Linux Security Update for wpa\_supplicant
- [503997](#) Alpine Linux Security Update for hostapd
- [504518](#) Alpine Linux Security Update for wpa\_supplicant
- [710136](#) Gentoo Linux hostapd and wpa\_supplicant Denial of service Vulnerability (GLSA 201908-25)
- [750549](#) OpenSUSE Security Update for wpa\_supplicant (openSUSE-SU-2020:2059-1)
- [750557](#) OpenSUSE Security Update for wpa\_supplicant (openSUSE-SU-2020:2053-1)
- [752179](#) SUSE Enterprise Linux Security Update for wpa\_supplicant (SUSE-SU-2022:1853-1)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)