



# CVE-2019-16275

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-16275
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-09-12 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:05:00 UTC
<b>Description</b>	hostapd before 2.10 and wpa_supplicant before 2.10 allow an incorrect indication of disconnection in certain situations beca

## Risk And Classification

**Problem Types:** CWE-346

## 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	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	8.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	W1.fi	Hostapd	All	All	All	All
Application	W1.fi	Wpa Supplicant	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 31 Update: hostapd-2.9-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: wpa_supplicant-2.8-3.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
w1.fi/security/2019-7/ap-mode-pmf-disconnection-protection-bypass.txt	MISC	<a href="https://w1.fi">w1.fi</a>
[SECURITY] Fedora 29 Update: wpa_supplicant-2.7-2.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] [DLA 1922-1] wpa security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 31 Update: wpa_supplicant-2.9-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
oss-security - Re: hostapd/wpa_supplicant: AP mode PMF disconnection protection bypass	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
[SECURITY] Fedora 31 Update: wpa_supplicant-2.9-2.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Index of /security/2019-7	MISC	<a href="https://w1.fi">w1.fi</a>
[SECURITY] Fedora 30 Update: hostapd-2.9-2.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-4538-1 wpa	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
[SECURITY] Fedora 29 Update: wpa_supplicant-2.7-2.fc29 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Bugtraq: [SECURITY] [DSA 4538-1] wpa security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>
[SECURITY] Fedora 30 Update: wpa_supplicant-2.8-3.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: hostapd-2.9-2.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
USN-4136-1: wpa_supplicant and hostapd vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
oss-security - hostapd/wpa_supplicant: AP mode PMF disconnection protection bypass	MISC	<a href="https://www.openwall.com">www.openwall.com</a>
USN-4136-2: wpa_supplicant and hostapd vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] Fedora 30 Update: hostapd-2.9-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[377146](#) Alibaba Cloud Linux Security Update for wpa\_supplicant (ALINUX3-SA-2021:0019)

[500248](#) Alpine Linux Security Update for hostapd

[500743](#) Alpine Linux Security Update for wpa\_supplicant

[503998](#) Alpine Linux Security Update for hostapd

[504522](#) Alpine Linux Security Update for wpa\_supplicant

[750549](#) OpenSUSE Security Update for wpa\_supplicant (openSUSE-SU-2020:2059-1)

[750557](#) OpenSUSE Security Update for wpa\_supplicant (openSUSE-SU-2020:2053-1)

750683 OpenSUSE Security Update for hostapd (openSUSE-SU-2021:0519-1)

900200 CBL-Mariner Linux Security Update for wpa\_supplicant 2.9

901136 Common Base Linux Mariner (CBL-Mariner) Security Update for wpa\_supplicant (6972-1)

903274 Common Base Linux Mariner (CBL-Mariner) Security Update for wpa\_supplicant (1816)

© [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](#)