



# CVE-2019-9495

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2019-9495  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cert@cert.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2019-04-17 14:29:00 UTC  |
| <b>Updated</b>         | 2023-11-07 03:13:00 UTC  |
| <b>Description</b>     | The implementations of EAP-PWD in hostapd and wpa_supplicant are vulnerable to side-channel attacks as a result of cac |

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                      | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 28      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 29      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 30      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 28      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 29      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 30      | All    | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | -      | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p2     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p3     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p4     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p5     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p6     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p7     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p8     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | p9     | All     | All      |
| Operating System | <a href="#">Freebsd</a>       | <a href="#">Freebsd</a>      | 11.2    | rc3    | All     | All      |

|                  |                          |                                |      |     |     |     |
|------------------|--------------------------|--------------------------------|------|-----|-----|-----|
| Operating System | <a href="#">Freebsd</a>  | <a href="#">Freebsd</a>        | 12.0 | -   | All | All |
| Operating System | <a href="#">Freebsd</a>  | <a href="#">Freebsd</a>        | 12.0 | p1  | All | All |
| Operating System | <a href="#">Freebsd</a>  | <a href="#">Freebsd</a>        | 12.0 | p2  | All | All |
| Operating System | <a href="#">Freebsd</a>  | <a href="#">Freebsd</a>        | 12.0 | p3  | All | All |
| Application      | <a href="#">Opensuse</a> | <a href="#">Backports Sle</a>  | 15.0 | -   | All | All |
| Application      | <a href="#">Opensuse</a> | <a href="#">Backports Sle</a>  | 15.0 | sp1 | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Leap</a>           | 15.1 | All | All | All |
| Application      | <a href="#">Synology</a> | <a href="#">Radius Server</a>  | 3.0  | All | All | All |
| Application      | <a href="#">Synology</a> | <a href="#">Router Manager</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 |

## References

| Reference   | Source  | Link  | Ta |
|---|---------|---|----|
| [SECURITY] Fedora 28 Update: hostapd-2.7-2.fc28 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |    |
| [SECURITY] Fedora 29 Update: hostapd-2.7-2.fc29 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |    |
| [security-announce] openSUSE-SU-2020:0222-1: moderate: Security update f                  | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           |    |
| Synology Inc.   | CONFIRM | <a href="http://www.synology.com">www.synology.com</a>                |    |
| [SECURITY] Fedora 30 Update: hostapd-2.7-2.fc30 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Ma |
| [SECURITY] [DLA 1867-1] wpa security update   | MLIST   | <a href="https://lists.debian.org">lists.debian.org</a>               |    |
| Index of /security/2019-2   | CONFIRM | <a href="#">w1.fi</a>   | Pe |
| [SECURITY] Fedora 29 Update: hostapd-2.7-2.fc29 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Ma |
| [SECURITY] Fedora 30 Update: hostapd-2.7-2.fc30 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |    |
| Bugtraq: FreeBSD Security Advisory FreeBSD-SA-19:03.wpa                                   | BUGTRAQ | <a href="https://seclists.org">seclists.org</a>                       |    |
| FreeBSD-SA-19:03  | FREEBSD | <a href="https://security.FreeBSD.org">security.FreeBSD.org</a>       |    |
| FreeBSD Security Advisory - FreeBSD-SA-19:03.wpa ≈ Packet Storm                           | MISC    | <a href="https://packetstormsecurity.com">packetstormsecurity.com</a> |    |
| [SECURITY] Fedora 28 Update: hostapd-2.7-2.fc28 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> | Ma |
| CVE Program record  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                          | ca |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                       | ca |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[44082](#) FortiOS-Dragonblood Vulnerabilities in WiFi WPA3 standard implementation (FG-IR-19-107)

[44092](#) FortiOS-Dragonblood Vulnerabilities in WiFi WPA3 standard implementation (FG-IR-19-107)

|   |
|---|
| <a href="#">500741</a> Alpine Linux Security Update for wpa_supplicant                                |
| <a href="#">504517</a> Alpine Linux Security Update for wpa_supplicant                                |
| <a href="#">750549</a> OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2020:2059-1)          |
| <a href="#">750557</a> OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2020:2053-1)          |
| <a href="#">752179</a> SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2022:1853-1) |

© [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](#)