



CVE-2019-9494

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

Summary

CVE	CVE-2019-9494
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-17 14:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	The implementations of SAE in hostapd and wpa_supplicant are vulnerable to side channel attacks as a result of observabl

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Freebsd	Freebsd	11.2	-	All	All
Operating System	Freebsd	Freebsd	11.2	p2	All	All
Operating System	Freebsd	Freebsd	11.2	p3	All	All
Operating System	Freebsd	Freebsd	11.2	p4	All	All
Operating System	Freebsd	Freebsd	11.2	p5	All	All
Operating System	Freebsd	Freebsd	11.2	p6	All	All
Operating System	Freebsd	Freebsd	11.2	p7	All	All
Operating System	Freebsd	Freebsd	11.2	p8	All	All
Operating System	Freebsd	Freebsd	11.2	p9	All	All
Operating System	Freebsd	Freebsd	11.2	rc3	All	All
Operating System	Freebsd	Freebsd	12.0	-	All	All

Operating System	Freebsd	Freebsd	12.0	p1	All	All
Operating System	Freebsd	Freebsd	12.0	p2	All	All
Operating System	Freebsd	Freebsd	12.0	p3	All	All
Application	Opensuse	Backports Sle	15.0	-	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Synology	Radius Server	3.0	All	All	All
Application	Synology	Router Manager	All	All	All	All
Application	W1.fi	Hostapd	All	All	All	All
Application	W1.fi	Wpa Supplicant	All	All	All	All

References

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

[500741](#) Alpine Linux Security Update for wpa_supplicant

[504517](#) Alpine Linux Security Update for wpa_supplicant

752177 SUSE Enterprise 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)

752179 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](#)