



# CVE-2017-13087

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

## Summary

<b>CVE</b>	CVE-2017-13087
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-10-17 13:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Group Temporal Key (GTK) whe

## Risk And Classification

**Problem Types:** CWE-330

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	17.04	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	17.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	10	All	All	All
Operating System	Freebsd	Freebsd	10.4	All	All	All
Operating System	Freebsd	Freebsd	11	All	All	All
Operating System	Freebsd	Freebsd	11.1	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	10	All	All	All

Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	10.4	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	11	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	11.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Point Of Sale</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Point Of Sale</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Openstack Cloud</a>	6	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Openstack Cloud</a>	6	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.2.4	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.2.5	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.2.6	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.2.8	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.3.10	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.3.11	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.3.7	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.3.9	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.4.10	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.4.11	All	All	All



Application	W1.fi	Hostapd	0.5.11	All	All	All
Application	W1.fi	Hostapd	0.5.7	All	All	All
Application	W1.fi	Hostapd	0.5.8	All	All	All
Application	W1.fi	Hostapd	0.5.9	All	All	All
Application	W1.fi	Hostapd	0.6.10	All	All	All
Application	W1.fi	Hostapd	0.6.8	All	All	All
Application	W1.fi	Hostapd	0.6.9	All	All	All
Application	W1.fi	Hostapd	0.7.3	All	All	All
Application	W1.fi	Hostapd	1.0	All	All	All
Application	W1.fi	Hostapd	1.1	All	All	All
Application	W1.fi	Hostapd	2.0	All	All	All
Application	W1.fi	Hostapd	2.1	All	All	All
Application	W1.fi	Hostapd	2.2	All	All	All
Application	W1.fi	Hostapd	2.3	All	All	All
Application	W1.fi	Hostapd	2.4	All	All	All
Application	W1.fi	Hostapd	2.5	All	All	All
Application	W1.fi	Hostapd	2.6	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.4	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.5	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.6	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.10	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.11	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.9	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.10	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.11	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.9	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.10	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.11	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.8	All	All	All

Application	W1.fi	Wpa Supplicant	0.5.9	All	All	All
Application	W1.fi	Wpa Supplicant	0.6.10	All	All	All
Application	W1.fi	Wpa Supplicant	0.6.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.6.9	All	All	All
Application	W1.fi	Wpa Supplicant	0.7.3	All	All	All
Application	W1.fi	Wpa Supplicant	1.0	All	All	All
Application	W1.fi	Wpa Supplicant	1.1	All	All	All
Application	W1.fi	Wpa Supplicant	2.0	All	All	All
Application	W1.fi	Wpa Supplicant	2.1	All	All	All
Application	W1.fi	Wpa Supplicant	2.2	All	All	All
Application	W1.fi	Wpa Supplicant	2.3	All	All	All
Application	W1.fi	Wpa Supplicant	2.4	All	All	All
Application	W1.fi	Wpa Supplicant	2.5	All	All	All
Application	W1.fi	Wpa Supplicant	2.6	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.4	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.5	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.6	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.2.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.10	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.11	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.3.9	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.10	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.11	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.4.9	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.10	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.11	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.7	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.8	All	All	All
Application	W1.fi	Wpa Supplicant	0.5.9	All	All	All
Application	W1.fi	Wpa Supplicant	0.6.10	All	All	All

Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	0.6.8	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	0.6.9	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	0.7.3	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	1.0	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	1.1	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	2.0	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	2.1	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	2.2	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	2.3	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	2.4	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	2.5	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	2.6	All	All	All

## References

### Reference

hostapd and wpa\_supplicant: Key Reinstallation (KRACK) attacks (GLSA 201711-03) — Gentoo Security

[w1.fi/security/2017-1/wpa-packet-number-reuse-with-replayed-message...](#)

[wpa\\_supplicant WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless Network -](#)

[ArubaOS WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless Network - Secur](#)

[FreeBSD-SA-17:07](#)

[Juniper Junos SRX Series WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless](#)

[Red Hat Customer Portal](#)

[Vulnerability Note VU#228519 - Wi-Fi Protected Access \(WPA\) handshake traffic can be manipulated to induce nonce and session key reuse](#)

[101274](#)

[Cisco IP Phones WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless Network](#)

[Android Security Bulletin—November 2017 | Android Open Source Project](#)

[\[security-announce\] openSUSE-SU-2017:2755-1: important: Security update](#)

[cert-portal.siemens.com/productcert/pdf/ssa-901333.pdf](#)

[Multiple Vulnerabilities in Wi-Fi Protected Access and Wi-Fi Protected Access II](#)

[Debian -- Security Information -- DSA-3999-1 wpa](#)

[Juniper ScreenOS WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless Network](#)

[USN-3455-1: wpa\\_supplicant and hostapd vulnerabilities | Ubuntu](#)

[Red Hat Customer Portal](#)

[KRACK Attacks: Breaking WPA2](#)

[\[security-announce\] SUSE-SU-2017:2745-1: important: Security update for](#)

[\[security-announce\] SUSE-SU-2017:2752-1: important: Security update for](#)

[www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt](http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt)

WPA2 Protocol Vulnerabilities - US

PEPPERL+FUCHS / ecom instruments WLAN enabled products utilizing WPA2 encryption (Update A) — English (USA)

KRACKs - wpa\_supplicant Multiple Vulnerabilities - Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[378244](#) Virtuozzo Linux Security Update for wpa\_supplicant (VZLSA-2017:2907)

[378248](#) Virtuozzo Linux Security Update for wpa\_supplicant (VZLSA-2017:2911)

[500246](#) Alpine Linux Security Update for hostapd

[500740](#) Alpine Linux Security Update for wpa\_supplicant

[503996](#) Alpine Linux Security Update for hostapd

[504516](#) Alpine Linux Security Update for wpa\_supplicant

[591394](#) ABB TropOS wireless mesh products WPA2 Key Reinstallation Multiple Vulnerabilities (ICSA-17-318-02A, ABBVU-PGGA-1KHW028907)

[710321](#) Gentoo Linux hostapd and wpa\_supplicant Key Reinstallation Vulnerability (GLSA 201711-03)

[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](#)**