CVE-2017-13078

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-13078
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-17 13:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the four-way hand

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	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	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7	All	All	All
Operating System	Redhat	Enterprise Linux Server	7	All	All	All
Operating System	Redhat	Enterprise Linux Server	7	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp3	All	All
Operating System	Suse	Linux Enterprise Point Of Sale	11	sp3	All	All
Operating System	Suse	Linux Enterprise Point Of Sale	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Openstack Cloud	6	All	All	All
Operating System	Suse	Openstack Cloud	6	All	All	All
Application	W1.fi	Hostapd	0.2.4	All	All	All
Application	W1.fi	Hostapd	0.2.5	All	All	All
Application	W1.fi	Hostapd	0.2.6	All	All	All
Application	W1.fi	Hostapd	0.2.8	All	All	All
Application	W1.fi	Hostapd	0.3.10	All	All	All
Application	W1.fi	Hostapd	0.3.11	All	All	All
Application	W1.fi	Hostapd	0.3.7	All	All	All
Application	W1.fi	Hostapd	0.3.9	All	All	All
Application	W1.fi	Hostapd	0.4.10	All	All	All
Application	W1.fi	Hostapd	0.4.11	All	All	All

Application	W1.fi	Hostapd	0.4.7	All	All	All
Application	W1.fi	Hostapd	0.4.8	All	All	All
Application	W1.fi	Hostapd	0.4.9	All	All	All
Application	W1.fi	Hostapd	0.5.10	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	Hostapd	0.2.4	All	All	All
Application	W1.fi	Hostapd	0.2.5	All	All	All
Application	W1.fi	Hostapd	0.2.6	All	All	All
Application	W1.fi	Hostapd	0.2.8	All	All	All
Application	W1.fi	Hostapd	0.3.10	All	All	All
Application	W1.fi	Hostapd	0.3.11	All	All	All
Application	W1.fi	Hostapd	0.3.7	All	All	All
Application	W1.fi	Hostapd	0.3.9	All	All	All
Application	W1.fi	Hostapd	0.4.10	All	All	All
Application	W1.fi	Hostapd	0.4.11	All	All	All
Application	W1.fi	Hostapd	0.4.7	All	All	All
Application	W1.fi	Hostapd	0.4.8	All	All	All
Application	W1.fi	Hostapd	0.4.9	All	All	All
Application	W1.fi	Hostapd	0.5.10	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	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

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
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple
About the security content of tvOS 11.1 - Apple Support
FreeBSD-SA-17:07
Oracle Critical Patch Update - January 2018
HPE Support document - HPE Support Center
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
Oracle Critical Patch Update - April 2018
Vulnerability Note VU#228519 - Wi-Fi Protected Access (WPA) handshake traffic can be manipulated to induce nonce and session key reuse
101274
About the security content of iOS 11.1 - Apple Support
Cisco IP Phones WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless Network
[SECURITY] [DLA 1573-1] firmware-nonfree security update
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

About the security content of watchOS 4.1 - Apple Support

Juniper ScreenOS WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless Networ

USN-3455-1: wpa_supplicant and hostapd vulnerabilities | Ubuntu

Red Hat Customer Portal

Fortinet FortiOS WPA/WPA2 Protocol Key Reinstallation Attack Lets Remote Users Access and Modify Data on the Target Wireless Network -

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

WPA2 Protocol Vulnerabilities - US

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

PHOENIX CONTACT WLAN enabled devices utilising WPA2 encryption (Update B) — 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

590571 PHOENIX CONTACT WLAN Capable Devices using the WPA2 Protocol Multiple Vulnerabilities (ICSA-17-325-01)

591073 Siemens SIMATIC RF350M and SIMATIC RF650M KRACK Attacks Multiple Vulnerabilities (SSA-418456)

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)