



CVE-2014-3686

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

Summary

CVE	CVE-2014-3686
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-16 00:55:00 UTC
Updated	2016-07-27 01:59:00 UTC
Description	wpa_supplicant and hostapd 0.7.2 through 2.2, when running with certain configurations and using wpa_cli or hostapd_cli v

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Application	W1.fi	Hostapd	0.7.2	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	0.7.2	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	Wpa Supplicant	0.72	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	0.72	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

References				
Reference	Source	Link		
hostapd and wpa_supplicant: Multiple vulnerabilities (GLSA 201606-17) — Gentoo Security	GENTOO	sec		
Bug 1151259 – CVE-2014-3686 wpa_supplicant and hostapd: wpa_cli and hostapd_cli remote command execution issue	CONFIRM	bug		
Index of /security/2014-1	CONFIRM	w1		
[security-announce] SUSE-SU-2014:1356-1: important: Security update for	SUSE	list		
Mageia Advisory: MGASA-2014-0429 - Updated wpa_supplicant and hostapd packages fix security vulnerability	CONFIRM	adv		
Debian -- Security Information -- DSA-3052-1 wpa	DEBIAN	ww		
Security Advisory SA60428 - Ubuntu update for wpa and wpasupplicant - Secunia	SECUNIA	sec		
USN-2383-1: wpa_supplicant vulnerability Ubuntu	UBUNTU	ww		
Red Hat Customer Portal	REDHAT	rhn		
Security Advisory SA61271 - SUSE update for wpa_supplicant - Secunia	SECUNIA	sec		
Security Advisory SA60366 - Debian update for wpa - Secunia	SECUNIA	sec		
wpa_supplicant and hostapd CVE-2014-3686 Remote Command Execution Vulnerability	BID	ww		
openSUSE-SU-2014:1313-1: moderate: update for wpa_supplicant	SUSE	list		
oss-security - wpa_cli and hostapd_cli action script execution vulnerability	MLIST	ww		
openSUSE-SU-2014:1314-1: moderate: update for wpa_supplicant	SUSE	list		
Support / Security / Advisories // MDVSA-2015:120 Mandriva	MANDRIVA	ww		
CVE Program record	CVE.ORG	ww		
ANNOUNCEMENT: CVE-2014-3686	ANNOUN			

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)