



# CVE-2015-4141

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

## Summary

<b>CVE</b>	CVE-2015-4141
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-06-15 15:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	The WPS UPnP function in hostapd, when using WPS AP, and wpa_supplicant, when using WPS external registrar (ER), 0

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Openseuse</a>	<a href="#">Openseuse</a>	13.1	All	All	All
Operating System	<a href="#">Openseuse</a>	<a href="#">Openseuse</a>	13.2	All	All	All
Operating System	<a href="#">Openseuse</a>	<a href="#">Openseuse</a>	13.1	All	All	All
Operating System	<a href="#">Openseuse</a>	<a href="#">Openseuse</a>	13.2	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.7.0	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.7.1	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.7.2	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.7.3	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	1.0	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	1.1	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	2.0	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	2.1	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	2.2	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	2.3	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	2.4	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.7.0	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	0.7.1	All	All	All

Application	W1.fi	Hostapd	0.7.2	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	Wpa Supplicant	0.7.0	All	All	All
Application	W1.fi	Wpa Supplicant	0.7.1	All	All	All
Application	W1.fi	Wpa Supplicant	0.7.2	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	0.7.0	All	All	All
Application	W1.fi	Wpa Supplicant	0.7.1	All	All	All
Application	W1.fi	Wpa Supplicant	0.7.2	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

## References

Reference	Source	Link
hostapd and wpa_supplicant: Multiple vulnerabilities (GLSA 201606-17) — Gentoo Security	GENTOO	<a href="#">security.gentoo.org</a>

© 2016-2017 Gentoo Linux, Inc. All rights reserved. This document is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

oss-security - CVE request: hostapd/wpa_supplicant - WPS UPnP vulnerability with HTTP chunked transfer encoding	MLIST	<a href="http://www.ubuntu.com">www.op</a>
USN-2650-1: wpa_supplicant and hostapd vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubi</a>
oss-security - Re: CVE request: vulnerability in wpa_supplicant and hostapd	MLIST	<a href="http://www.ubuntu.com">www.op</a>
openSUSE-SU-2015:1030-1: moderate: Recommended update for wpa_supplicant	SUSE	<a href="http://lists.opensuse.org">lists.ope</a>
Debian -- Security Information -- DSA-3397-1 wpa	DEBIAN	<a href="http://www.debian.org">www.del</a>
w1.fi/security/2015-2/wps-upnp-http-chunked-transfer-encoding.txt	CONFIRM	<a href="http://w1.fi">w1.fi</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[750549](#) OpenSUSE Security Update for wpa\_supplicant (openSUSE-SU-2020:2059-1)

[750557](#) OpenSUSE Security Update for wpa\_supplicant (openSUSE-SU-2020:2053-1)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)