



CVE-2015-5316

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

Summary

CVE	CVE-2015-5316
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-21 16:29:00 UTC
Updated	2018-03-21 13:06:00 UTC
Description	The eap_pwd_perform_confirm_exchange function in eap_peer/eap_pwd.c in wpa_supplicant 2.x before 2.6, when EAP-pv

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	W1.fi	Wpa Supplicant	All	All	All	All
Application	W1.fi	Wpa Supplicant	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - wpa_supplicant: EAP-pwd peer error path failure on unexpected Confirm message	MLIST	www.openwall.com	Malware
USN-2808-1: wpa_supplicant and hostapd vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Broken
w1.fi/security/2015-8/eap-pwd-unexpected-confirm.txt	CONFIRM	w1.fi	Mitigation
Malformed Request	BID	www.securityfocus.com	Threat
Debian -- Security Information -- DSA-3397-1 wpa	DEBIAN	www.debian.org	Threat
CVE Program record	CVE.ORG	www.cve.org	Card
NVD vulnerability detail	NVD	nvd.nist.gov	Card

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](#)