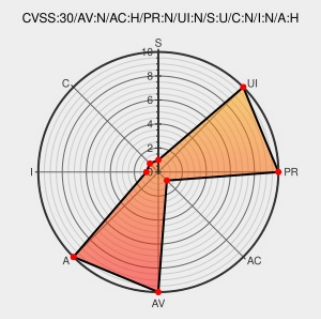
CVE-2015-5314

Published on: 02/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5314

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

The eap_pwd_process function in eap_server/eap_server_pwd.c in hostapd 2.x before 2.6 does not validate that the reassembly buffer is large enough for the final fragment when used with (1) an internal EAP server or (2) a RADIUS server and EAP-pwd is enabled in a runtime configuration, which allows remote attackers to cause a denial of service (process termination) via a large final fragment in an EAP-pwd message.

CVE-2015-5314 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
USN-2808-1: wpa_supplicant and hostapd vulnerabilities | Ubuntu	Broken Link www.ubuntu.com	UBUNTU USN-2808-1

	text/html	
oss-security - hostapd/wpa_supplicant: EAP-pwd missing last fragment length validation	Mailing List Mitigation Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20151110 hostapd/wpa_supplicant: EAP-pwd missing last fragment length validation
	Mitigation Vendor Advisory w1.fi text/plain	CONFIRM w1.fi/security/2015-7/eap-pwd-missing-last-fragment-length-validation.txt
Debian -- Security Information -- DSA-3397-1 wpa	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3397

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:*:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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