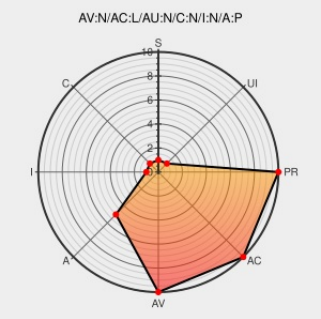
CVE-2015-4144

Published on: 06/15/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:07 PM UTC

CVE-2015-4144

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



Certain versions of Opensuse from Opensuse contain the following vulnerability:

The EAP-pwd server and peer implementation in hostapd and wpa_supplicant 1.0 through 2.4 does not validate that a message is long enough to contain the Total-Length field, which allows remote attackers to cause a denial of service (crash) via a crafted message.

CVE-2015-4144 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
	Vendor Advisory, w1.fi, text/plain	CONFIRM w1.fi/security/2015-4/eap-pwd-missing-payload-length-validation.txt
hostapd and wpa_supplicant: Multiple vulnerabilities (GLSA 201606-17) — Gentoo Security	Third Party Advisory, security.gentoo.org, text/html	GENTOO GLSA-201606-17
USN-2650-1: wpa_supplicant and hostapd vulnerabilities | Ubuntu	www.ubuntu.com, text/html	UBUNTU USN-2650-1
oss-security - Re: CVE request: vulnerability in wpa_supplicant and hostapd	www.openwall.com, text/html	MLIST [oss-security] 20150531 Re: CVE request: vulnerability in wpa_supplicant and hostapd
openSUSE-SU-2015:1030-1: moderate: Recommended update for wpa_supplicant	Third Party Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2015:1030

oss-security - Re: CVE request: vulnerability in wpa_supplicant and hostapd	www.openwall.com text/html	MLIST [oss-security] 20150509 Re: CVE request: vulnerability in wpa_supplicant and hostapd
Debian -- Security Information -- DSA-3397-1 wpa	www.debian.org Depreciated Link text/html	DEBIAN DSA-3397

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	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	2.3	All	All	All
Application	W1.fi	Hostapd	2.4	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	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	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

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:2.2:*:*:*:*:*:*:*:

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

cpe:2.3:a:w1.fi:hostapd:2.4:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:hostapd:2.2:*:*:*:*:*:*:*:

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

cpe:2.3:a:w1.fi:hostapd:2.4:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:2.2:*:*:*:*:*:*:*:

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

cpe:2.3:a:w1.fi:wpa_supplicant:2.4:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:w1.fi:wpa_supplicant:2.2:*:*:*:*:*:*:*:

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

cpe:2.3:a:w1.fi:wpa_supplicant:2.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→