CVE-2015-1863

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-1863
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-28 14:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Heap-based buffer overflow in wpa_supplicant 1.0 through 2.4 allows remote attackers to cause a denial of service (crash),

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

AV:A/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:A/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All

Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
[security-announce] openSUSE-SU-2015:0813-1: important: Security update	af854a3a-2127-422b-91ae-36
Red Hat Customer Portal	af854a3a-2127-422b-91ae-36
hostapd and wpa_supplicant: Multiple vulnerabilities (GLSA 201606-17) — Gentoo Security	af854a3a-2127-422b-91ae-36
Full Disclosure: [ALICLOUDSEC-VUL2015-001]Android wpa_supplicant WLAN Direct remote buffer overflow	af854a3a-2127-422b-91ae-36
wpa_supplicant P2P SSID Parsing Flaw May Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-36
USN-2577-1: wpa_supplicant vulnerability | Ubuntu	af854a3a-2127-422b-91ae-36
w1.fi/security/2015-1/wpa_supplicant-p2p-ssid-overflow.txt	af854a3a-2127-422b-91ae-36
wpa_supplicant CVE-2015-1863 Heap Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-36
阿里巴巴集团安全应急响应中心	af854a3a-2127-422b-91ae-36
Android wpa_supplicant Heap Overflow ≈ Packet Storm	af854a3a-2127-422b-91ae-36
Debian -- Security Information -- DSA-3233-1 wpa	af854a3a-2127-422b-91ae-36

Debian -- Security Information -- DSA-3233-1 wpa	af854a3a-2127-422b-91ae-36
SecurityFocus	af854a3a-2127-422b-91ae-36
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**