CVE-2005-0470

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

Summary

CVE	CVE-2005-0470
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-03-14 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in wpa_supplicant before 0.2.7 allows remote attackers to cause a denial of service (segmentation fault) via

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	All	All	All	All

Operating System	Suse	Suse Linux	9.2	All	All	All
Operating System	Suse	Suse Linux	9.2	All	x86_64	All
Application	Wpa Supplicant	Wpa Supplicant	0.2	All	All	All
Application	Wpa Supplicant	Wpa Supplicant	0.2.1	All	All	All
Application	Wpa Supplicant	Wpa Supplicant	0.2.2	All	All	All
Application	Wpa Supplicant	Wpa Supplicant	0.2.3	All	All	All
Application	Wpa Supplicant	Wpa Supplicant	0.2.4	All	All	All
Application	Wpa Supplicant	Wpa Supplicant	0.2.5	All	All	All
Application	Wpa Supplicant	Wpa Supplicant	0.2.6	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a-2127-4
Secunia - Advisories - wpa_supplicant EAPOL-Key Frames Buffer Overflow	af854a3a-2127-4
SecurityTracker.com Archives - wpa_supplicant Key Data Length Missing Validation Lets Remote Users Crash the Service	af854a3a-2127-4
Gentoo Linux Documentation -- wpa_supplicant: Buffer overflow vulnerability	af854a3a-2127-4
wpa_supplicant - new stable releases v0.3.8 and v0.2.7	af854a3a-2127-4
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.