CVE-2021-30004

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-30004
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-02 05:15:00 UTC
Updated	2023-09-30 11:15:00 UTC
Description	In wpa_supplicant and hostapd 2.9, forging attacks may occur because AlgorithmIdentifier parameters are mishandled in tls

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	W1.fi	Hostapd	2.9	All	All	All
Application	W1.fi	Wpa Supplicant	2.9	All	All	All

References

Reference	Source	Link	Tags
hostap - hostapd/wpa_supplicant	MISC	w1.fi	
wpa_supplicant, hostapd: Multiple Vulnerabilities (GLSA 202309-16) — Gentoo security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

174886 SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2021:1125-1)

174891 SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2021:1166-1)

500250 Alpine Linux Security Update for hostapd

500746 Alpine Linux Security Update for wpa_supplicant

501507 Alpine Linux Security Update for wpa_supplicant

501792 Alpine Linux Security Update for wpa_supplicant

504000 Alpine Linux Security Update for hostapd

504521 Alpine Linux Security Update for wpa_supplicant

710760 Gentoo Linux wpa_supplicant, hostapd Multiple Vulnerabilities (GLSA 202309-16)

750264 OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2021:0563-1)

750683 OpenSUSE Security Update for hostapd (openSUSE-SU-2021:0519-1)

900255 CBL-Mariner Linux Security Update for wpa_supplicant 2.9

901937 Common Base Linux Mariner (CBL-Mariner) Security Update for wpa_supplicant (6974-1)

903590 Common Base Linux Mariner (CBL-Mariner) Security Update for wpa_supplicant (4051)