CVE-2020-3922

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

Summary

CVE	CVE-2020-3922
State	PUBLIC
Assigner	cve@cert.org.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-18 07:15:00 UTC
Updated	2020-03-19 19:15:00 UTC
Description	LisoMail, by ArmorX, allows SQL Injections, attackers can access the database without authentication via a URL parameter

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Armorx	Lisomail	All	All	All	All

References

Reference	Source	Link
TWCERT/CC台灣電腦網路危機處理暨協調中心-ArmorX LisoMail電子郵件協同作業 - SQL Injection	MISC	www.t
CHT Security Discovered a Pre-Auth SQL Injection in Well-known Email System | 中華資安國際 CHT Security Co., Ltd.	MISC	www.c
ArmorX Webmail Pre-Auth SQL Injection.md · GitHub	MISC	gist.git
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

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