



CVE-2022-27904

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-27904
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-01 00:15:00 UTC
Updated	2023-02-09 02:11:00 UTC
Description	Automox Agent for macOS before version 39 was vulnerable to a time-of-check/time-of-use (TOCTOU) race-condition attack

Risk And Classification

Problem Types: CWE-367

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Application	Automox	Automox	All	All	All	All

References

Reference	Source	Link	Tags
Automox: IT Operations Cloud Solution No VPNs, No Hassle	MISC	automox.com	
Automox Known Product Security Vulnerabilities	MISC	www.automox.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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