



CVE-2021-26909

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

Summary

CVE	CVE-2021-26909
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-23 16:15:00 UTC
Updated	2022-04-26 16:03:00 UTC
Description	Automox Agent prior to version 31 uses an insufficiently protected S3 bucket endpoint for storing sensitive files, which could

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Automox	Automox	All	All	All	All

References

Reference	Source
CVE-2021-26908 & 26909: Automox Agent Info Disclosure Rapid7 Blog	MIS
CVE-2021-26908 and CVE-201-26909: Automox Agent Information Disclosure Vulnerabilities [Fixed] - Automox - Automox Community	COM
CVE Program record	CVE
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Danny Jordan of Rapid7, and disclosed in accordance with Rapid7's vulnerability disclosure policy at <https://www.rapid7.com/security/disclosure#zeroday>

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)