



CVE-2021-42192

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

Summary

CVE	CVE-2021-42192
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-04 11:15:00 UTC
Updated	2023-11-07 22:15:00 UTC
Description	Konga v0.14.9 is affected by an incorrect access control vulnerability where a specially crafted request can lead to privilege

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Konga Project	Konga	0.14.9	All	All	All

References

Reference	Source	Link
KONGA 0.14.9 - Privilege Escalation - Multiple webapps Exploit	MISC	www.exploit
Fix listing size and added pagination to consumer groups. Ref issue #302 · pantsel/konga@d615352 · GitHub		github.com
GitHub - pantsel/konga: More than just another GUI to Kong Admin API	MISC	github.com
Security Advisory for Konga v.14.9 - Google Docs	MISC	docs.goog
GitHub - whokilleddb/Konga-Privilege-Escalation-Exploit: Authenticated Privilege Escalation In Konga API Gateway	MISC	github.com
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

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](#)