



CVE-2021-32849

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

Summary

CVE	CVE-2021-32849
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-26 22:15:00 UTC
Updated	2022-02-02 19:32:00 UTC
Description	Gerapy is a distributed crawler management framework. Prior to version 0.9.9, an authenticated user could execute arbitrar

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Security Issue: GHSL-2021-076-gerapy · Issue #217 · Gerapy/Gerapy · GitHub	MISC	github.com
GHSL-2021-076: Arbitrary command execution in Gerapy - CVE-2021-32849 GitHub Security Lab	MISC	securitylab.github.com
GitHub Security Lab: Security Contact Needed · Issue #197 · Gerapy/Gerapy · GitHub	MISC	github.com
Gerapy < 0.9.9 An authenticated user can execute arbitrary command · Advisory · Gerapy/Gerapy · GitHub	CONFIRM	github.com
Problem loading page	MISC	lgtm.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)