



CVE-2023-0475

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

Summary

CVE	CVE-2023-0475
State	PUBLIC
Assigner	security@hashicorp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-16 19:15:00 UTC
Updated	2023-02-27 18:33:00 UTC
Description	HashiCorp go-getter up to 1.6.2 and 2.1.1 is vulnerable to decompression bombs. Fixed in 1.7.0 and 2.2.0.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hashicorp	Go-getter	2.1.1	All	All	All
Application	Hashicorp	Go-getter	All	All	All	All

References

Reference	Source	Link
HCSEC-2023-4 - go-getter vulnerable to denial of service via malicious compressed archive - Security - HashiCorp Discuss	MISC	discuss.hashicorp.com
CVE Program record	CVE.ORG	cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[905564](#) Common Base Linux Mariner (CBL-Mariner) Security Update for k3s (13572)

[905568](#) Common Base Linux Mariner (CBL-Mariner) Security Update for packer (13586)

[905575](#) Common Base Linux Mariner (CBL-Mariner) Security Update for terraform (13606)

[907815](#) Common Base Linux Mariner (CBL-Mariner) Security Update for packer (13586-1)

© [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](#)