



CVE-2022-1996

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-1996
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-08 13:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	Authorization Bypass Through User-Controlled Key in GitHub repository emicklei/go-restful prior to v3.8.0.

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Go-restful Project	Go-restful	All	All	All	All

References

Reference	Source	L
[SECURITY] Fedora 35 Update: golang-github-emicklei-restful-3.8.0-1.fc35 - package-announce - Fedora Mailing-Lists		lic
[SECURITY] Fedora 36 Update: golang-github-chromedp-0.8.1-2.fc36 - package-announce - Fedora Mailing-Lists		lic
[SECURITY] Fedora 36 Update: golang-oras-0.15.1-1.20221105git690716b.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lic
[SECURITY] Fedora 36 Update: golang-github-emicklei-restful-3.8.0-1.fc36 - package-announce - Fedora Mailing-Lists		lic
[SECURITY] Fedora 36 Update: aquatone-1.7.0-7.fc36 - package-announce - Fedora Mailing-Lists		lic
CVE-2022-1996 go-restful Vulnerability in NetApp Products NetApp Product Security	CONFIRM	sc
[SECURITY] Fedora 35 Update: golang-github-emicklei-restful-3.8.0-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lic
[SECURITY] Fedora 36 Update: golang-github-chromedp-0.8.1-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lic
[SECURITY] Fedora 36 Update: golang-oras-0.15.1-1.20221105git690716b.fc36 - package-announce - Fedora Mailing-Lists		lic
[SECURITY] Fedora 36 Update: golang-github-emicklei-restful-3.8.0-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lic
[SECURITY] Fedora 38 Update: golang-helm-3-3.11.1-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lic
[SECURITY] Fedora 37 Update: golang-oras-0.15.1-1.20221105git690716b.fc37 - package-announce - Fedora Mailing-Lists		lic

[SECURITY] Fedora 37 Update: golang-oras-0.15.1-1.20221105git690716b.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lis
[SECURITY] Fedora 36 Update: aquatone-1.7.0-7.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lis
Authorization Bypass Through User-Controlled Key vulnerability found in go-restful	CONFIRM	hi
use exact matching of allowed domain entries, issue #489 (#493) · emicklei/go-restful@fd3c327 · GitHub	MISC	gi
[SECURITY] Fedora 37 Update: golang-oras-0.15.1-1.20221105git690716b.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lis
[SECURITY] Fedora 35 Update: fzf-0.29.0-2.fc35 - package-announce - Fedora Mailing-Lists		lis
[SECURITY] Fedora 35 Update: fzf-0.29.0-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lis
[SECURITY] Fedora 38 Update: golang-helm-3-3.11.1-1.fc38 - package-announce - Fedora Mailing-Lists		lis
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184280 Debian Security Update for golang-github-emicklei-go-restful (CVE-2022-1996)
282858 Fedora Security Update for golang (FEDORA-2022-589a0ad690)
282859 Fedora Security Update for golang (FEDORA-2022-185697ef56)
282893 Fedora Security Update for 3mux (FEDORA-2022-fae3ecee19)
282931 Fedora Security Update for apptainer (FEDORA-2022-ba365d3703)
282947 Fedora Security Update for 3mux (FEDORA-2022-3969b64d4b)
283049 Fedora Security Update for fzf (FEDORA-2022-30c5ed5625)
283739 Fedora Security Update for golang (FEDORA-2023-6550d9323b)
283740 Fedora Security Update for golang (FEDORA-2023-c9b2182a4e)
284277 Fedora Security Update for golang (FEDORA-2023-4e2068ba5d)
284299 Fedora Security Update for etcd (FEDORA-2022-28d38313c8)
354064 Amazon Linux Security Advisory for golist : ALAS2-2022-1847
354067 Amazon Linux Security Advisory for golang : ALAS2-2022-1846
354069 Amazon Linux Security Advisory for golang : ALAS-2022-1635
354083 Amazon Linux Security Advisory for runc : ALAS2DOCKER-2022-020
354088 Amazon Linux Security Advisory for golang-github-syndtr-gocapability : ALAS2-2022-1865
354089 Amazon Linux Security Advisory for golang-googlecode-sqlite : ALAS2-2022-1862
354090 Amazon Linux Security Advisory for golang-github-kr-pty : ALAS2-2022-1864

354091 Amazon Linux Security Advisory for go-rpm-macros : ALAS2-2022-1863

354092 Amazon Linux Security Advisory for golang-googlecode-net : ALAS2-2022-1861

354093 Amazon Linux Security Advisory for golang-github-gorilla-mux : ALAS2-2022-1860

354094 Amazon Linux Security Advisory for golang-github-gorilla-context : ALAS2-2022-1859

354096 Amazon Linux Security Advisory for golang-github-godbus-dbus : ALAS2-2022-1858

354370 Amazon Linux Security Advisory for golang-github-cpuguy83-md2man : ALAS2022-2022-140

354493 Amazon Linux Security Advisory for golist : ALAS2022-2022-133

354504 Amazon Linux Security Advisory for golist : ALAS2022-2022-192

354527 Amazon Linux Security Advisory for golang : ALAS2022-2022-193

354566 Amazon Linux Security Advisory for golang : ALAS-2022-193

503184 Alpine Linux Security Update for gitlab-runner

506077 Alpine Linux Security Update for gitlab-runner

753059 SUSE Enterprise Linux Security Update for helm (SUSE-SU-2022:4606-1)

753186 SUSE Enterprise Linux Security Update for kubevirt (SUSE-SU-2022:3333-1)

753204 SUSE Enterprise Linux Security Update for helm (SUSE-SU-2022:3666-1)

753213 SUSE Enterprise Linux Security Update for kubevirt (SUSE-SU-2022:3321-1)

753225 SUSE Enterprise Linux Security Update for cdi-apiserver-container (SUSE-SU-2022:3334-1)

753403 SUSE Enterprise Linux Security Update for cdi-apiserver-container (SUSE-SU-2022:3335-1)

755442 SUSE Enterprise Linux Security Update for catatonit, containerd, runc (SUSE-SU-2023:4727-1)

904867 Common Base Linux Mariner (CBL-Mariner) Security Update for helm (12350)

904961 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-containerd (12363)

904976 Common Base Linux Mariner (CBL-Mariner) Security Update for cert-manager (12463)

905001 Common Base Linux Mariner (CBL-Mariner) Security Update for k3s (12503)

905011 Common Base Linux Mariner (CBL-Mariner) Security Update for prometheus (12607)

905046 Common Base Linux Mariner (CBL-Mariner) Security Update for rook (12626)

905055 Common Base Linux Mariner (CBL-Mariner) Security Update for keda (12507)

905074 Common Base Linux Mariner (CBL-Mariner) Security Update for containerized-data-importer (12480)

905083 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-containerd (12566)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)