



CVE-2021-3121

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

Summary

CVE	CVE-2021-3121
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-11 06:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	An issue was discovered in GoGo Protobuf before 1.3.2. plugin/unmarshal/unmarshal.go lacks certain index validation, aka

Risk And Classification

Problem Types: CWE-129

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Protobuf	All	All	All	All
Application	Golang	Protobuf	All	All	All	All
Application	Hashicorp	Consul	All	All	All	All
Application	Hashicorp	Consul	All	All	All	All

References

Reference	Source
Pony Mail!	MLIST
CVE-2021-3121 GoGo Protobuf Vulnerability in NetApp Products NetApp Product Security	CONFIRM
[skywalking-notifications] 20211018 [GitHub] [skywalking-swck] hanahmily opened a new pull request #37: Fix vulnerabilities	
[pulsar-commits] 20210121 [GitHub] [pulsar-client-go] hrsakai opened a new pull request #446: Upgrade gogo/protobuf to 1.3.2	
Comparing v1.3.1...v1.3.2 · gogo/protobuf · GitHub	MISC
HCSEC-2021-23 - Consul Exposed to Denial of Service in GoGo Protobuf Dependency - Security - HashiCorp Discuss	MISC
skippy peanut butter · gogo/protobuf@b03c65e · GitHub	MISC
Pony Mail!	MLIST
[pulsar-commits] 20210122 [GitHub] [pulsar-client-go] hrsakai opened a new pull request #446: Upgrade gogo/protobuf to 1.3.2	
Pony Mail!	MLIST

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179912](#) Debian Security Update for golang-gogoprotobuf (CVE-2021-3121)

[239212](#) Red Hat Update for OpenShift Container Platform 4.7.5 (RHSA-2021:1006)

[239525](#) Red Hat Update for OpenShift Container Platform 4.8.2 (RHSA-2021:2437)

[501764](#) Alpine Linux Security Update for protobuf-c

[504321](#) Alpine Linux Security Update for protobuf-c

[770055](#) Red Hat OpenShift Container Platform 4.7.5 Security and Bug Fix Update (RHSA-2021:1006)

[770064](#) Red Hat OpenShift Container Platform 4.7.0 Packages and Security Update (RHSA-2020:5634)

[770074](#) Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:2437)

[770109](#) Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-1006)

[770111](#) Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-2437)

© [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](#)