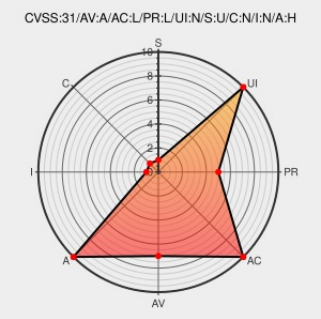
CVE-2022-1941

Published on: Not Yet Published

Last Modified on: 10/01/2022 02:27:00 AM UTC

CVE-2022-1941

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Protobuf-cpp from Google contain the following vulnerability:

A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-python can lead to out of memory failures. A specially crafted message with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated.

CVE-2022-1941 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
oss-security - CVE-2022-1941: Protobuf C++, Python DoS	www.openwall.com text/html	MLIST [oss-security] 20220927 CVE-2022-1941: Protobuf C++, Python DoS
A potential Denial of Service issue in protobuf-cpp and protobuf-python · Advisory · protocolbuffers/protobuf · GitHub	github.com text/html	CONFIRM github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf
Security Bulletins | Customer Care | Google Cloud	cloud.google.com text/html	CONFIRM cloud.google.com/support/bulletins#GCP-2022-019

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

752777 SUSE Enterprise Linux Security Update for protobuf (SUSE-SU-2022:3922-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Protobuf-cpp	All	All	All	All
Application	Google	Protobuf-python	All	All	All	All

cpe:2.3:a:google:protobuf-cpp:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:protobuf-python:*:*:*:*:*:*:*:*:

Discovery Credit

CluterFuzz - https://google.github.io/clusterfuzz/

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-1941 : A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and includ… twitter.com/i/web/status/1…	2022-09-22 14:55:29
@JohnJasonFallow	New vulnerability on the NVD: CVE-2022-1941 ift.tt/B1TYSw4	2022-09-22 16:16:49
@doogsineerg	New vulnerability on the NVD: CVE-2022-1941 ift.tt/p0LaS3g	2022-09-22 16:33:23
@workentin	New vulnerability on the NVD: CVE-2022-1941 ift.tt/4brMRkV	2022-09-22 16:40:11
@xanadulinux	CVE-2022-1941 ift.tt/bXoEQ8J	2022-09-22 16:52:31
@LinInfoSec	Python - CVE-2022-1941: cloud.google.com/support/bullet…	2022-09-22 17:01:13
/r/netcve	CVE-2022-1941	2022-09-22 15:38:21

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report