



# CVE-2022-3171

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

## Summary

<b>CVE</b>	CVE-2022-3171
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-10-12 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:50:00 UTC
<b>Description</b>	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Application	<a href="#">Google</a>	<a href="#">Google-protobuf</a>	All	All	All	All
Application	<a href="#">Google</a>	<a href="#">Protobuf-java</a>	All	All	All	All
Application	<a href="#">Google</a>	<a href="#">Protobuf-javalite</a>	All	All	All	All
Application	<a href="#">Google</a>	<a href="#">Protobuf-kotlin</a>	All	All	All	All
Application	<a href="#">Google</a>	<a href="#">Protobuf-kotlin-lite</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 37 Update: protobuf-3.19.6-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
A potential Denial of Service issue in protobuf-java · Advisory · protocolbuffers/protobuf · GitHub	CONFIRM	<a href="#">github.com</a>
[SECURITY] Fedora 36 Update: perl-Alien-ProtoBuf-0.09-17.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
protobuf-java: Denial of Service (GLSA 202301-09) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
[SECURITY] Fedora 37 Update: protobuf-3.19.6-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: perl-Alien-ProtoBuf-0.09-17.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[20317](#) Oracle Database 21c Critical Patch Update - January 2023

[20318](#) Oracle Database 19c Critical Patch Update - January 2023

[20319](#) Oracle Database 19c Critical OJVM Patch Update - January 2023

[20391](#) IBM DB2 Denial of Service (DoS) Vulnerability (7087234)

[283528](#) Fedora Security Update for protobuf (FEDORA-2022-25f35ed634)

[284287](#) Fedora Security Update for perl (FEDORA-2022-15729fa33d)

[355269](#) Amazon Linux Security Advisory for protobuf : ALAS2023-2023-049

[377910](#) Oracle MySQL Connectors 8.0.x Denial of Service (DoS) Vulnerability (CPUJAN2023)

[378553](#) IBM MQ Blockchain bridge Denial of Service (DoS) Vulnerability within protobuf-java core (6853381)

[378733](#) IBM WebSphere Application Server Liberty Denial of Service (DoS) Vulnerability (6841889)

[378776](#) IBM MQ Denial of Service (DoS) Vulnerabilities (6960535)

[378883](#) Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

[378990](#) Atlassian Jira Service Management Data Center and Server Denial of Service (DoS) Vulnerability (JSDSERVER-14749,JSDSERVER-14751,JSDSERVER-14752,JSDSERVER-14753,JSDSERVER-14754,JSDSERVER-14755)

[691034](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (dc49f6dc-99d2-11ed-86e9-d4c9ef517024)

[710705](#) Gentoo Linux protobuf-java Denial of Service (DoS) Vulnerability (GLSA 202301-09)

[731313](#) Atlassian Jira Software Data Center and Server Denial of Service (DoS) Vulnerability (JSWSERVER-25789)

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

[754157](#) SUSE Enterprise Linux Security Update for grpc, protobuf, python-Deprecated, python-PyGithub, python-aiocontextvars, python-avro, python-bcrypt, python-cryptography, python-cryptography-vectors, python-google-api-core, pyt (SUSE-SU-2023:2783-1)

[754878](#) SUSE Enterprise Linux Security Update for grpc, protobuf, python-DEPRECATED, python-PyGithub, python-aiocontextvars, python-avro, python-bcrypt, python-cryptography, python-cryptography-vectors, python-google-api-core, pyt (SUSE-SU-2023:2783-2)

© [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](#).

