



# CVE-2019-13132

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

## Summary

<b>CVE</b>	CVE-2019-13132
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-10 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:03:00 UTC
<b>Description</b>	In ZeroMQ libzmq before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.3.2, a remote, unauthenticated client connecting to a

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Application	<a href="#">Zeromq</a>	<a href="#">Libzmq</a>	All	All	All	All
Application	<a href="#">Zeromq</a>	<a href="#">Libzmq</a>	All	All	All	All

## References

Reference	Source	Link
ZeroMQ libzmq CVE-2019-13132 Stack Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] Fedora 31 Update: zeromq-4.3.2-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: zeromq-4.3.2-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
oss-security - CVE-2019-13132: zeromq/libzmq: denial of service via stack overflow with arbitrary data	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Releases · zeromq/libzmq · GitHub	CONFIRM	<a href="http://github.com">github.com</a>
[security-announce] openSUSE-SU-2019:1767-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 31 Update: zeromq-4.3.2-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
ZeroMQ: Arbitrary code execution (GLSA 201908-17) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
Debian -- Security Information -- DSA-4477-1 zeromq3	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
[SECURITY] Fedora 29 Update: zeromq-4.1.7-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
USN-4050-1: ZeroMQ vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>
Bugtraq: [SECURITY] [DSA 4477-1] zeromq3 security update	BUGTRAQ	<a href="http://seclists.org">seclists.org</a>
CVE-2019-13132: denial of service via stack overflow · Issue #3558 · zeromq/libzmq · GitHub	CONFIRM	<a href="http://github.com">github.com</a>
[SECURITY] [DLA 1849-1] zeromq3 security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 29 Update: zeromq-4.1.7-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: zeromq-4.3.2-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[500829](#) Alpine Linux Security Update for zeromq

[504566](#) Alpine Linux Security Update for zeromq

[690129](#) Free Berkeley Software Distribution (FreeBSD) Security Update for libzmq4 (6954a2b0-bda8-11eb-a04e-641c67a117d8)

[710143](#) Gentoo Linux ZeroMQ Arbitrary code execution Vulnerability (GLSA 201908-17)

© 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](https://status.cve.report)**