



CVE-2020-15166

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

Summary

CVE	CVE-2020-15166
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-11 16:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	In ZeroMQ before version 4.3.3, there is a denial-of-service vulnerability. Users with TCP transport public endpoints, even v

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Zeromq	Libzmq	All	All	All	All
Application	Zeromq	Libzmq	All	All	All	All

References

Reference	Source	Li
[SECURITY] Fedora 32 Update: zeromq-4.3.3-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lis
[SECURITY] Fedora 33 Update: zeromq-4.3.3-1.fc33 - package-announce - Fedora Mailing-Lists		lis
ZeroMQ: Denial of service (GLSA 202009-12) — Gentoo security	GENTOO	se
problem: zeromq connects peer before handshake is complete by somdoron · Pull Request #3913 · zeromq/libzmq · GitHub	MISC	git
Problem: test_security_zap occasionally segfaults by bluca · Pull Request #3973 · zeromq/libzmq · GitHub	MISC	git
[SECURITY] [DLA 2443-1] zeromq3 security update	MLIST	lis
[SECURITY] Fedora 32 Update: zeromq-4.3.3-1.fc32 - package-announce - Fedora Mailing-Lists		lis
[SECURITY] Fedora 33 Update: zeromq-4.3.3-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lis
Denial-of-Service on CURVE/ZAP-protected servers by unauthenticated clients · Advisory · zeromq/libzmq · GitHub	CONFIRM	git

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500830](#) Alpine Linux Security Update for zeromq

[504567](#) Alpine Linux Security Update for zeromq

[690130](#) Free Berkeley Software Distribution (FreeBSD) Security Update for libzmq4 (21ec4428-bdaa-11eb-a04e-641c67a117d8)

[750605](#) OpenSUSE Security Update for zeromq (openSUSE-SU-2020:1910-1)

[750608](#) OpenSUSE Security Update for zeromq (openSUSE-SU-2020:1907-1)

© [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](#)