



CVE-2020-15254

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

Summary

CVE	CVE-2020-15254
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-16 17:15:00 UTC
Updated	2022-08-05 19:30:00 UTC
Description	Crossbeam is a set of tools for concurrent programming. In crossbeam-channel before version 0.4.4, the bounded channel

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Crossbeam Project	Crossbeam	All	All	All	All
Application	Crossbeam Project	Crossbeam	All	All	All	All

References

Reference
Add advisory for UB in crossbeam-channel 0.4.3 by taiki-e · Pull Request #425 · RustSec/advisory-db · GitHub
Memory Leak in crossbeam-queue ArrayQueue? (Latest git only, ver0.2.3 is not effected) · Issue #539 · crossbeam-rs/crossbeam · GitHub
Use Box<T> instead of Vec<T> to initialize and drop ArrayQueue by caelunshun · Pull Request #533 · crossbeam-rs/crossbeam · GitHub
Undefined Behavior in bounded channel · Advisory · crossbeam-rs/crossbeam · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500955](#) Alpine Linux Security Update for firefox

[503840](#) Alpine Linux Security Update for firefox

© [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](#)