



CVE-2018-21232

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

Summary

CVE	CVE-2018-21232
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-29 14:15:00 UTC
Updated	2020-05-14 12:15:00 UTC
Description	re2c before 2.0 has uncontrolled recursion that causes stack consumption in find_fixed_tags.

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Re2c	Re2c	All	All	All	All
Application	Re2c	Re2c	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - re2c: infinite loop	MISC	www.openwall.com	Mailing List, Third Party
oss-security - Re: re2c: infinite loop	MLIST	www.openwall.com	
overflow-1.re test fails on system with small stack · Issue #219 · skvadrik/re2c · GitHub	MISC	github.com	Exploit, Patch, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[691040](#) Free Berkeley Software Distribution (FreeBSD) Security Update for re2c (b0e1fa2b-9c86-11ed-9296-002b67dfc673)

[900868](#) Common Base Linux Mariner (CBL-Mariner) Security Update for re2c (7337)

[907323](#) Common Base Linux Mariner (CBL-Mariner) Security Update for re2c (7337-1)

© [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](#)