



CVE-2020-5235

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

Summary

CVE	CVE-2020-5235
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-04 03:15:00 UTC
Updated	2020-02-06 18:51:00 UTC
Description	There is a potentially exploitable out of memory condition in Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is cor

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Fix invalid free() after failed realloc() (GHSA-gcx3-7m76-287p) · nanopb/nanopb@7b39682 · GitHub	MISC	github.com	Patc
Out-of-memory condition on repeated field can result in invalid free() · Advisory · nanopb/nanopb · GitHub	CONFIRM	github.com	Patc
Fix invalid free() after failed realloc() (GHSA-gcx3-7m76-287p) · nanopb/nanopb@45582f1 · GitHub	MISC	github.com	Patc
Fix invalid free() after failed realloc() (GHSA-gcx3-7m76-287p) · nanopb/nanopb@aa9d0d1 · GitHub	MISC	github.com	Patc
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[610329](#) Google Pixel Android April 2021 Security Patch Missing

[610347](#) Google Android May 2021 Security Patch Missing for Huawei EMUI

© [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](#)