



CVE-2021-22156

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-22156
State	PUBLIC
Assigner	secure@blackberry.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-17 19:15:00 UTC
Updated	2021-08-30 11:26:00 UTC
Description	An integer overflow vulnerability in the calloc() function of the C runtime library of affected versions of BlackBerry® QNX So

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Blackberry	Qnx Os For Medical	All	All	All	All
Operating System	Blackberry	Qnx Os For Safety	All	All	All	All
Application	Blackberry	Qnx Software Development Platform	All	All	All	All
Application	Blackberry	Qnx Software Development Platform	6.5.0	-	All	All
Application	Blackberry	Qnx Software Development Platform	6.5.0	sp1	All	All

References

Reference

- BlackBerry QNX-2021-001 Vulnerability Affecting Cisco Products: August 2021
- QNX-2021-001 Vulnerability in the C Runtime Library Impacts BlackBerry QNX Software Development Platform (SDP), QNX OS for Medical, e
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)