



CVE-2021-35093

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

Summary

CVE	CVE-2021-35093
State	PUBLIC
Assigner	product-security@qualcomm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-03 08:15:00 UTC
Updated	2022-01-13 17:35:00 UTC
Description	Possible memory corruption in BT controller when it receives an oversized LMP packet over 2-DH1 link and leads to denial

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Qualcomm	Csr8510 A10	-	All	All	All
Operating System	Qualcomm	Csr8510 A10 Firmware	-	All	All	All
Hardware	Qualcomm	Csr8811 A12	-	All	All	All
Operating System	Qualcomm	Csr8811 A12 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
December 2021 Security Bulletin Qualcomm	CONFIRM	www.qualcomm.com	
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.

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

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](#)