



CVE-2019-14204

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

Summary

CVE	CVE-2019-14204
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-31 13:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply h

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Denx	U-boot	All	All	All	All

References

Reference	Source	Link	Tags
U-Boot NFS RCE Vulnerabilities (CVE-2019-14192) - GitHub Security Lab	MISC	blog.semmle.com	Third Party Advisory
u-boot / u-boot · GitLab	MISC	gitlab.com	Third Party Advisory
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

[671381](#) EulerOS Security Update for uboot-tools (EulerOS-SA-2022-1312)

[671382](#) EulerOS Security Update for uboot-tools (EulerOS-SA-2022-1296)

[750595](#) OpenSUSE Security Update for u-boot (openSUSE-SU-2020:1930-1)

© [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](#)