



CVE-2019-2114

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

Summary

CVE	CVE-2019-2114
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-11 19:15:00 UTC
Updated	2019-10-25 19:15:00 UTC
Description	In the default privileges of NFC, there is a possible local bypass of user interaction requirements on package installation du

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	8.0	All	All	All
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All
Operating System	Google	Android	8.0	All	All	All
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All

References

Reference	Source	Link
NFC Beaming Bypasses Security Controls in Android [CVE-2019-2114] Nightwatch Cybersecurity	MISC	www.nightwatchcybersec
Android Security Bulletin—October 2019 Android Open Source Project	CONFIRM	source.android.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)