

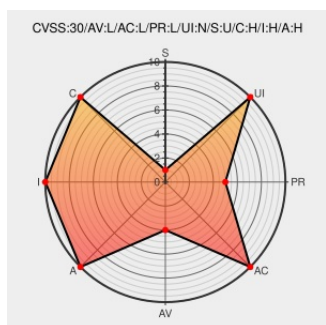


CVE-2018-9518

Published on: 12/07/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:54 PM UTC

CVE-2018-9518

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

In `nfc_llcp_build_sdreq_tlv` of `llcp_commands.c`, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-73083945.

CVE-2018-9518 has been assigned by security@android.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Google Inc.** - **Android** version **Android Kernel**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
USN-3798-1: Linux kernel vulnerabilities Ubuntu security	Patch	UBUNTU USN-3798-1

notices | Ubuntu

Third Party Advisory

usn.ubuntu.com

text/html

USN-3798-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices

Third Party Advisory

usn.ubuntu.com

text/html

UBUNTU USN-3798-2

Pixel/Nexus Security Bulletin—September 2018

Vendor Advisory

source.android.com

text/html

 CONFIRM

source.android.com/security/bulletin/pixel/2018-09-01

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:google:android:-:*:*:*:*:*:						
cpe:2.3:o:google:android:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)