



Published on: Not Yet Published

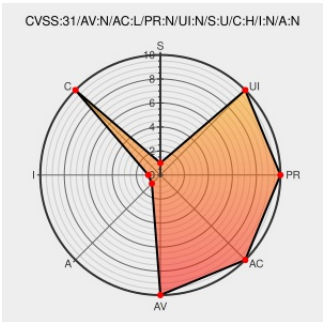
Last Modified on: 09/08/2023 04:26:00 PM UTC

CVE-2023-33914

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

In NIA0 algorithm in Security Mode Command, there is a possible missing verification incorrect input. This could lead to remote information disclosure no additional execution privileges needed

CVE-2023-33914 has been assigned by security@unisoc.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software:  **Unisoc (Shanghai) Technologies Co., Ltd. - T760/T770/T820/S8000** version = **Android13/Android11/Android12**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
This page could not be found	www.unisoc.com text/html Inactive Link Not Archived	 MISC www.unisoc.com/en_us/secy/announcementDetail/www.unisoc.com/en_us/secy/announcementDe

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.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	11.0	-	All	All
Operating System	Google	Android	12.0	-	All	All
Operating System	Google	Android	13.0	-	All	All
Hardware  	Unisoc	S8000	-	All	All	All
Hardware  	Unisoc	T760	-	All	All	All
Hardware  	Unisoc	T770	-	All	All	All
Hardware  	Unisoc	T820	-	All	All	All
cpe:2.3:o:google:android:11.0:-:*****:						
cpe:2.3:o:google:android:12.0:-:*****:						
cpe:2.3:o:google:android:13.0:-:*****:						
cpe:2.3:h:unisoc:s8000:-:*****:						
cpe:2.3:h:unisoc:t760:-:*****:						
cpe:2.3:h:unisoc:t770:-:*****:						
cpe:2.3:h:unisoc:t820:-:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© 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