



CVE-2023-25954

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

Summary

CVE	CVE-2023-25954
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-13 04:15:00 UTC
Updated	2023-04-21 17:54:00 UTC
Description	KYOCERA Mobile Print' v3.2.0.230119 and earlier, 'UTAX/TA MobilePrint' v3.2.0.230119 and earlier, and 'Olivetti Mobile P

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kyocera	Mobile Print	All	All	All	All
Application	Olivetti	Mobile Print	All	All	All	All
Application	Triumph-adler	Mobile Print	All	All	All	All

References

Reference	Source	Link
Olivetti Mobile Print - Apps on Google Play	MISC	play.google.com
JVNVU#98434809: Multiple mobile printing apps for Android vulnerable to improper intent handling	MISC	jvn.jp
TA/UTAX Mobile Print - Apps on Google Play	MISC	play.google.com
KYOCERA Mobile Print for Android Security Vulnerability KYOCERA Document Solutions	MISC	www.kyoceradocumentsolu
KYOCERA Mobile Print - Apps on Google Play	MISC	play.google.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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)