



CVE-2022-27648

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-27648
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-29 19:15:00 UTC
Updated	2023-04-05 16:36:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on affected installations of KOYO Screen Creator 0.1.1.

Risk And Classification

Problem Types: CWE-121

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jtekt	Screen Creator Advance 2	All	All	All	All
Application	Jtekt	Screen Creator Advance 2	0.1.1.4	-	All	All
Application	Jtekt	Screen Creator Advance 2	0.1.1.4	build01	All	All
Application	Jtekt	Screen Creator Advance 2	0.1.1.4	build01b	All	All
Application	Jtekt	Screen Creator Advance 2	0.1.1.4	build02	All	All

References

Reference	Source	Link
[Update notice] Screen Creator Advance 2 software of GC-A2 Series KOYO ELECTRONICS INDUSTRIES CO., LTD.	MISC	www.koyoelectronics.com
ZDI-22-543 Zero Day Initiative	MISC	www.zerodayinitiative.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](#)