



CVE-2021-42704

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

Summary

CVE	CVE-2021-42704
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-18 17:15:00 UTC
Updated	2022-10-14 11:47:00 UTC
Description	Inkscape version 0.91 is vulnerable to an out-of-bounds write, which may allow an attacker to arbitrary execute code.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Inkscape	Inkscape	0.91	All	All	All

References

Reference	Source	Link	Tags
Inkscape in Industrial Products CISA	CONFIRM	www.cisa.gov	
SCADA Animation Graphic Editor Extension for Inkscape 1+ - Ecava IGX Web SCADA	CONFIRM	www.integraxor.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

LEGACY: Tran Van Khang – khangkito (VinCSS), working with Trend Micro's Zero Day Initiative, reported these vulnerabilities to CISA.

Legacy QID Mappings

[179396](#) Debian Security Update for inkscape (CVE-2021-42704)

[355090](#) Amazon Linux Security Advisory for inkscape : ALAS2-2023-2043

© [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](#)