



CVE-2023-27249

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

Summary

CVE	CVE-2023-27249
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-23 02:15:00 UTC
Updated	2023-03-27 15:59:00 UTC
Description	swfdump v0.9.2 was discovered to contain a heap buffer overflow in the function swf_GetPlaceObject at swfobject.c.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Swftools	Swftools	0.9.2	All	All	All

References

Reference	Source	Link
poc/poc at main · keepinggg/poc · GitHub	MISC	keepinggg/poc
poc/poc_of_swfdump at main · keepinggg/poc · GitHub	MISC	keepinggg/poc
SWF Dump	MISC	swfdump
GitHub - matthiaskramm/swftools: Utilities for editing and generating Adobe Flash (SWF) files.	MISC	matthiaskramm/swftools
heap-buffer-overflow exists in the function swf_GetPlaceObject in swfobject.c · Issue #197 · matthiaskramm/swftools · GitHub	MISC	matthiaskramm/swftools
CVE Program record	CVE.ORG	CVE-2023-27249
NVD vulnerability detail	NVD	CVE-2023-27249

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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