



CVE-2023-26876

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

Summary

CVE	CVE-2023-26876
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-21 15:15:00 UTC
Updated	2023-04-28 16:15:00 UTC
Description	SQL injection vulnerability found in Piwigo v.13.5.0 and before allows a remote attacker to execute arbitrary code via the filt

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Piwigo	Piwigo	All	All	All	All

References

Reference	Source	Link	Tags
Piwigo 13.5.0 SQL Injection ~ Packet Storm	MISC	packetstormsecurity.com	
Full Disclosure: Piwigo - CVE-2023-26876	FULLDISC	seclists.org	
Piwigo - Image library software and Digital Asset Management	MISC	piwigo.com	
POC - Authenticated SQL injection Piwigo 13.5.0 - CVE-2023-26876 · GitHub	MISC	gist.github.com	
Tempest – Home	MISC	www.tempest.com.br	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)