



CVE-2020-8089

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

Summary

CVE	CVE-2020-8089
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-10 16:15:00 UTC
Updated	2020-02-14 16:50:00 UTC
Description	Piwigo 2.10.1 is affected by stored XSS via the Group Name Field to the group_list page.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Piwigo	Piwigo	2.10.1	All	All	All
Application	Piwigo	Piwigo	2.10.1	All	All	All

References

Reference	Source	Link	Tags
Stored Cross-Site Scripting vulnerability in Piwigo CMS · Issue #1150 · Piwigo/Piwigo · GitHub	CONFIRM	github.com	Exploit, Issue Tr
Announcements Piwigo.org	MISC	piwigo.org	Release Notes,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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

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