



WordPress Google Photos Gallery with Shortcodes Plugin <= 4.0.2 is vulnerable to Cross Site Scripting (XSS)

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

Summary

CVE	CVE-2023-51373
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-29 11:15:09 UTC
Updated	2026-04-28 19:22:42 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ian Kennerley Google

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

EPSS: 0.001670000 probability, percentile 0.372960000 (date 2026-05-06)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope
Changed
Confidentiality
Low
Integrity
Low
Availability
None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nakunakifi	Google Photos Gallery With Shortcodes	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ian Kennerley	Google Photos Gallery With Shortcodes	affected n/a 4.0.2 custom	Not specified

References

Reference	Source
WordPress Google Photos Gallery with Shortcodes plugin <= 4.0.2 - Reflected Cross Site Scripting (XSS) vulnerability - Patchstack	af854a3
CVE Program record	CVE.OF
NVD vulnerability detail	NVD



Vendor Comments And Credit

Discovery Credit
CNA: Le Ngoc Anh (Patchstack Alliance) (en)

Additional Advisory Data

Solutions
CNA: Update to 4.0.3 or a higher version.

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

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