



# WordPress Robo Gallery Plugin <= 3.2.17 is vulnerable to Cross Site Scripting (XSS)

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

## Summary

<b>CVE</b>	CVE-2024-22295
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-31 18:15:49 UTC
<b>Updated</b>	2026-04-28 19:23:15 UTC
<b>Description</b>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RoboSoft Photo Galler

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000510000 probability, percentile 0.156520000 (date 2026-04-28)

**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	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/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	<a href="#">Robogallery</a>	<a href="#">Robo Gallery</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">RoboSoft</a>	<a href="#">Photo Gallery Images Slider In Rbs Image Gallery</a>	affected n/a 3.2.17 custom	Not specified

#### References

Reference	Source
WordPress Robo Gallery plugin <= 3.2.17 - Cross Site Scripting (XSS) vulnerability - Patchstack	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Bryan Satyamulya (Patchstack Alliance) (en)

#### Additional Advisory Data

Solutions

**CNA:** Update to 3.2.18 or a higher version.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)