



# Lychee Vulnerable to Stored XSS via Photo Description in RSS/Atom/JSON Feed (No Sanitization on Public Endpoint)

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

## Summary

<b>CVE</b>	CVE-2026-33738
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 21:17:08 UTC
<b>Updated</b>	2026-03-30 18:45:14 UTC
<b>Description</b>	Lychee is a free, open-source photo-management tool. Prior to version 7.5.3, the photo `description` field is stored without I

## Risk And Classification

**Primary CVSS:** v4.0 4.8 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:L/VA:N/SC:H/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000590000 probability, percentile 0.185240000 (date 2026-04-01)

**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
4.0	security-advisories@github.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:L/VA:N/SC:H/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:L/VA:N/SC:H/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

High

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:L/VA:N/SC:H/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### 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	Lycheeorg	Lychee	All	All	All	All

### Vendor Declared Affected Products

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">LycheeOrg</a>	<a href="#">Lychee</a>	affected < 7.5.3	Not specified

References

Reference	Source	Link
<a href="https://github.com/LycheeOrg/Lychee/security/advisories/GHSA-5574-7f3r-hm9j">github.com/LycheeOrg/Lychee/security/advisories/GHSA-5574-7f3r-hm9j</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="#">github</a>
<a href="https://github.com/LycheeOrg/Lychee/releases/tag/v7.5.3">github.com/LycheeOrg/Lychee/releases/tag/v7.5.3</a>	security-advisories@github.com	<a href="#">github</a>
<a href="https://github.com/LycheeOrg/Lychee/pull/4218">github.com/LycheeOrg/Lychee/pull/4218</a>	security-advisories@github.com	<a href="#">github</a>
<a href="https://github.com/LycheeOrg/Lychee/commit/d2e2606a0223d5a384d5b806db1b31eb587adc5c">github.com/LycheeOrg/Lychee/commit/d2e2606a0223d5a384d5b806db1b31eb587adc5c</a>	security-advisories@github.com	<a href="#">github</a>
CVE Program record	CVE.ORG	<a href="#">www.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

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](#)**