contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

jdownloads.com jDownloads extension for Joomla: new CVE

CVE-2026-117551 · record published 12 November 2026

Analysis Report

If you run the jDownloads extension on a Joomla site below version 4.1.8, update now. The fixed release, jDownloads 4.1.8 Stable, came out on 12 November 2026. If you do not use jDownloads, or ...

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/jdownloads-com-jdownloads-extension-for-cve-2026-117551

The bottom line

> *If you run the jDownloads extension on a Joomla site below version 4.1.8, update now. The fixed release, jDownloads 4.1.8 Stable, came out on 12 November 2026. If you do not use jDownloads, or already run 4.1.8 or later, there is nothing to do here.*

At a glance

Fact	Detail
Product	jdownloads.com jDownloads extension for Joomla (CVE-2026-117551)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by Joomla on 12 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 13 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	jDownloads 4.1.8 Stable, released 12 November 2026 per the vendor's news page.
Who looks first	Anyone running Joomla sites that use the jDownloads download-manager extension, especially where registered or front-end users are allowed to upload files or thumbnails.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run the jDownloads extension on any Joomla site?	Nothing to do for this CVE.	Check the installed version (next question).
Is the installed jDownloads version below 4.1.8?	You are on the fixed release; nothing to do.	You are in range; see the next question.
Can registered or front-end users upload files or thumbnails?	Much lower risk; update at your normal patch cycle.	Treat as higher priority and update now.

What it is

The record says a user who already has permission to upload could place an executable file on the server through the front-end thumbnail upload, because those uploads were not properly checked. That lets them run PHP code on the server.

Why it matters

The flaw needs an account that can already upload, so it is not open to anonymous visitors. Our reading is that it still matters because many Joomla sites let registered users upload downloads or thumbnails, and this turns that limited permission into running code on the server. The record gives it the maximum score of 10. The vendor's news page says 4.1.8 fixes several security issues at once, so updating closes more than this one flaw.

What the vendor's advisory says

We read one page on www.jdownloads.com. In short:

- The vendor's news page says version 4.1.8, created 12 November 2026, fixes multiple security issues and addresses file and image handling, permission checks for referenced downloads, external download URL processing and access to administrative functionality.
- It adds checks on renaming files already assigned to a download; a renamed main or preview file must keep its extension, and to change the type you re-upload through the normal workflow.
- External downloads that need an HTTP redirect during server-side retrieval may now be rejected; the vendor advises using a direct file URL where possible.
- The vendor says to take a full backup of the site and database before updating, install through Joomla's extension installer, then re-check the upload, editing and download workflows.
- The vendor notes the update does not rotate existing scan keys; if a scan key may have been exposed, rotate it and update any scheduled URL-based scan jobs.

Things people will get wrong

- Anyone on the internet can run code on our server. The record says the attacker must already hold upload permission, so it needs an account that can upload, not an anonymous visitor.
- Only the thumbnail image is at risk. The record says the weak thumbnail upload lets an executable file be placed and PHP code run, so the server itself is at risk, not just images.

How we would triage it

This is our judgement.

Step 1: Find which sites and versions you run

- List the jDownloads version installed on each Joomla site you manage, because only versions below 4.1.8 are in range.
- Note which of those sites let front-end or registered users upload, as those carry more risk.

Step 2: Reduce exposure until you update

- Until you update, limit who can upload files and thumbnails in jDownloads to trusted administrators, since the flaw needs upload permission.
- Review recent uploads for unexpected PHP or executable files in the jDownloads upload folders.

Step 3: Update to the fixed release

- Take a full backup of the site and database, then install jDownloads 4.1.8 through Joomla's extension installer, as the vendor advises.
- The vendor says 4.1.8 fixes several security issues, so this closes more than this one flaw.

Step 4: Check after updating

- Confirm the version now reads 4.1.8 or later.
- The vendor says the update does not rotate scan keys; if a scan key may have been exposed, rotate it and update scheduled URL-based scan jobs.
- Re-test your upload, editing and download workflows, as the vendor recommends.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we are checking our exposure to a security issue in the jDownloads download-manager extension for Joomla, recorded as CVE-2026-117551. Could you confirm in writing whether we run jDownloads on any of our Joomla sites, and if so on which sites and which version? Versions below 4.1.8 are affected. The fixed release is jDownloads 4.1.8 Stable, published on 12 November 2026. Please update any affected site to 4.1.8 or later, taking a full backup first, and confirm back to us the version found and that the update has been applied. We would like written confirmation by the end of next week. Thank you.*

The weakness behind it

The record classes this as CWE-434.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The record describes a web-facing upload feature in a Joomla extension that lets a permitted user place an executable file and run code, so exploiting an internet-facing application's weakness would likely fit.
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	Exploitation needs an account that already holds upload permission, so an attacker would likely use a valid or registered account to reach the vulnerable feature.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The flaw ends in running PHP code on the server, so an attacker would likely use the server's scripting interpreter to execute their uploaded file.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *Joomla Extension - jdownloads.com - RCE through file upload in jDownloads < 4.1.8 - Insufficient validation of frontend thumbnail uploads allowed users with upload permission to place executable files on the server. This results in PHP code execution.*

Versions of jdownloads.com jDownloads extension for Joomla the record lists as affected:

- 1.0.0-4.1.7

The record gives no version ranges. Use the vendor's advisory for the affected versions.

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-117551
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-117551
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The record does not say whether any site has actually been attacked through this flaw.
- It does not state which jDownloads upload settings or permission levels leave a site reachable.
- The vendor's news page does not map its listed fixes to this CVE, so which specific change addresses this flaw is not stated.
- No workaround other than updating is given; whether restricting upload permission fully removes the risk is not said.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 13 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-117551: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:A/AU:Y` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
12 November 2026	CVE record published by Joomla.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
A public Joomla site on jDownloads below 4.1.8 that lets registered or front-end users upload files or thumbnails	Medium	this week

A jDownloads site below 4.1.8 where only trusted administrators can upload	Low	next patch cycle
A site already running jDownloads 4.1.8 or later, or not using jDownloads at all	None	none for this CVE

Appendix 4. Definition of done

- Every jdownloads.com jDownloads extension for Joomla you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-117551: https://www.cve.org/CVERecord?id=CVE-2026-117551
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.jdownloads.com: https://www.jdownloads.com/