



# **DJ-HelpfulArticles 1.3 fixes a stored XSS anyone could plant in the admin overview**

DJ-HelpfulArticles 1.3 fixes CVE-2026-102800, a stored XSS in the Joomla rating widget: a visitor-supplied IP was saved unchecked and shown to admins.

Phil E. Taylor | 27 October 2026

On 27 October 2026 DJ-Extensions published DJ-HelpfulArticles 1.3: Security Update, a security release for its free Joomla article-rating extension. The vendor rates the flaw High, classes it as stored cross-site scripting (CWE-79), and credits Ala Arfaoui with the report. No CVE had been assigned when it was released.

DJ-HelpfulArticles puts a one-click “was this helpful?” widget under an article, lets an unhappy reader leave a reason, and shows the administrator statistics on what was rated. The flaw sits where the two meet. Any visitor, with no account, could submit script through the rating widget, and that script could run in an administrator’s browser the next time they opened the overview. The post below is our reading of the vendor’s advisory, not of the code.

## Update, 27 October 2026: CVE-2026-102800, scored 8.7 High

The Joomla CNA published CVE-2026-102800 for this flaw a few hours after the release and scored it CVSS 4.0 8.7 High, against our 8.6 High. The record credits Ala Arfaoui and lists DJ-HelpfulArticles 1.0.0 to 1.2.0 as affected, wider than the advisory’s “version 1.2”, so mySites.guru now flags every version below 1.3 for this CVE. The fix is still 1.3.

## TL;DR

- The rating widget accepted a **visitor IP address supplied by the browser** and stored it without checking it was an IP address
- The value was **escaped for the database but not for HTML**, so the administrator’s “Helpful articles” overview printed it raw
- An **unauthenticated** visitor could plant JavaScript that ran with an **administrator’s session** when the overview was opened

- **1.3 fixes it:** the IP now comes from the connection's REMOTE\_ADDR and is validated, and stored values in the overview are escaped before rendering
- Updating **does not delete** values already planted; the vendor's FAQ says so
- The vendor names **version 1.2**. Versions 1.0.0 to 1.1.0 have a separate XSS, [CVE-2024-27183](#), so every release below 1.3 has a known XSS of one kind or another
- Published as [CVE-2026-102800](#), scored **8.7 High** by the Joomla CNA. We score it **8.6 High** on CVSS 4.0. This is DJ-Extensions' fix

# 8.7

CVSS 4.0

## CVE-2026-102800 Unauthenticated stored XSS through the visitor IP field

**HIGH** Joomla CNA

An anonymous visitor plants script through the rating widget's IP field, and it runs in an administrator's browser session when the Helpful articles overview is opened.

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

No login needed to plant it

CWE-79 stored XSS

Fixed in 1.3

### ▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

#### How it is reached

AV:N Network: Reachable across the internet

AC:L Low: Nothing to work around, it just works

AT:N None: Works against any affected install

PR:N None: No account needed

UI:P Passive: Someone has to visit a page

#### What it does to the site

VC:H High: Everything the site holds can be read

VI:H High: Data and files can be altered at will

VA:H High: The site can be taken down

#### What it does beyond the site

SC:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

# 8.6

CVSS 4.0

## DJ-HelpfulArticles 1.2: unauthenticated stored XSS through the visitor IP field (our assessment)

**HIGH** mySites.guru assessment

An anonymous visitor submits a rating with script in place of an IP address. The record waits in the database until an administrator opens the Helpful articles overview, at which point the script runs with that

administrator's session and can do anything the administrator can do through the browser, such as create a new administrator account or install an extension.

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N

No login needed to plant it

Fires when an admin opens the overview

Fixed in 1.3

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

#### How it is reached

AV:N Network: Reachable across the internet

AC:L Low: Nothing to work around, it just works

AT:N None: Works against any affected install

PR:N None: No account needed

UI:A Active: Someone has to be talked through a few steps

#### What it does to the site

VC:H High: Everything the site holds can be read

VI:H High: Data and files can be altered at will

VA:L Low: The site slows or stutters

#### What it does beyond the site

SC:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

## How the DJ-HelpfulArticles rating widget trusted the wrong IP address

The widget records which visitor rated which article, and it used the visitor's IP address to do that. Before 1.3, that IP address was part of the data the browser sent along with the rating. The server took the value as given and stored it, with no check that it was an IPv4 or IPv6 address, or an address at all. Anyone who can submit a rating can edit the request before it leaves their machine, so the "IP address" field was in practice a free-text field open to the public.

Storing it did no harm on its own, because the value was escaped on the way into the database. Where it went wrong was on the way out. The administrator's "Helpful articles" overview displayed the stored IP without HTML escaping, so a value such as a script tag was written straight into the page and the browser ran it.

That is the classic stored XSS shape. Escaping for the database protects the SQL query from the value; escaping for HTML protects the page from it. Doing one does not do the other, so a string that was safe to store was dangerous to print.

The damage depends on who opens the page. Script running in a logged-in Joomla administrator's browser has that administrator's session, so it can do whatever the administrator can do through the browser: create a new Super User, install an extension, change a template file. The attacker does not need to log in. They submit one rating and wait for an administrator to look at the statistics, which is what the extension is for.

## What changed in DJ-HelpfulArticles 1.3

DJ-Extensions describes the fix in two parts: where the IP address comes from, and how stored values are shown.

On the input side, all three AJAX handlers (helpful ratings, not-helpful ratings and feedback reasons) now read the visitor IP from the connection's REMOTE\_ADDR and validate it. The IP that the browser used to send in the request data is no longer used, and forwarded IP headers are ignored too. IP handling was removed from the widget JavaScript altogether, so a current rating request simply does not include one.

On the output side, the admin overview now escapes stored IP addresses, article titles, feedback reasons and displayed dates before rendering them. That last part is what makes the overview safe to open even when old records hold something nasty.

The vendor says its tests covered forged IP values, IPv4 and IPv6 addresses, invalid connection addresses, and safe rendering of stored malicious content. We have not tested the release ourselves and we are not publishing a payload.

## Which DJ-HelpfulArticles versions are affected?

The advisory says to update every installation running version 1.2. It does not say whether versions before 1.2 share this flaw, so for 1.1.0 and earlier the answer is "unstated".

It does not much matter, because those versions have a known XSS of their own. [CVE-2024-27183](#), published on 9 July 2024 and rated Medium, is a separate cross-site scripting flaw in DJ-HelpfulArticles 1.0.0 to 1.1.0. Put the two together and every release below 1.3 has a published XSS of one kind or another. The fixed version is 1.3 for all of them.

## What to do about DJ-HelpfulArticles on your Joomla sites

1. Update to 1.3. Download it from [DJ-Extensions](#) (it is free, but you need an account) or take it from the Joomla updater if your site offers it, then confirm the installed version under System, Manage, Extensions.
2. Check what was already stored. The vendor's FAQ is clear that updating does not delete previously stored malicious values. Once you are on 1.3 the overview is escaped and safe to open, so open it and read down the IP column. Anything that is not an IP address was put there by hand. Remove those ratings and feedback records.
3. Check for what the script might have done. If any administrator opened the overview while the site was on 1.2 and a planted record was waiting, treat the admin session as possibly used. Look for administrator accounts you did not create and extensions you did not install. We have a [walkthrough on finding rogue admin accounts in Joomla](#).
4. If you find either, the site has been compromised and the clean-up is bigger than this extension. Start with our [Joomla hacked guide](#).

## Find administrator accounts you never created

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

### Updating does not clean out what was already stored

DJ-HelpfulArticles 1.3 stops stored values executing in the admin overview. It does not remove them. A record planted while the site ran 1.2 is still in the database after the update, and a site that updates and never looks at the overview has patched the display and kept the evidence. Open it once on 1.3 and check the IP column.

## How mySites.guru flags DJ-HelpfulArticles

We added this flaw to the mySites.guru [vulnerability database](#) on 27 October 2026, and widened the rule to the CVE record's 1.0.0 to 1.2.0 range when [CVE-2026-102800](#) was published, so any connected Joomla site running DJ-HelpfulArticles below 1.3 is flagged on its dashboard. Sites on 1.1.0 and below are also flagged for [CVE-2024-27183](#).

From there it is one job rather than a site-by-site hunt. The flagged sites can be updated in a batch with the [mass updater](#), and the rogue admin check above runs on every connected site as part of the full audit, so a new Super User you did not create shows up in a report instead of in a client's complaint. That is how we handle advisories across a [portfolio of Joomla sites](#), and it is part of every subscription.

## Why a visitor IP address is an XSS vector in more Joomla extensions than this one

DJ-HelpfulArticles is rare among the Joomla sites connected to mySites.guru: none of them currently run it. We are writing it up anyway, because the shape of the flaw is far more common than the extension.

An IP address only comes from one trustworthy place: the TCP connection, which PHP exposes as `REMOTE_ADDR`. Anything else, whether a field in the request body or a header like `X-Forwarded-For`, is written by the client and can say whatever the client likes. The one legitimate exception is a site behind a proxy it trusts, which may read the forwarded header, and then only from that proxy. An extension that reads the IP from the request body is reading attacker-controlled text and labelling it as a network fact, which is how a field no developer thought of as “input” ends up holding a script tag.

The second half of the pattern is just as common. Public AJAX endpoints that record something (a vote, a view, a form submission, a user agent) and then list those records to an administrator are everywhere in Joomla extensions, and they are exactly the surface we described in our post on [AJAX endpoints as the CMS security blind spot](#). The visitor-facing side gets attention because it is visible. The admin list that displays what the visitor sent is an afterthought, and the escaping on it is the first thing to be missed. Any extension on your sites that stores a visitor IP or user agent and shows it in an admin screen deserves the same question this one has now answered.

DJ-Extensions has had a busy year on this front: in July 2026 it released a security update for DJ-Classifieds after we reported an [unauthenticated file upload](#), a different class of flaw in a different product. Both times it published a security release post that said what changed, instead of an unannounced patch.

If you look after more than a handful of Joomla sites, knowing which of them run an extension named in an advisory is most of the job, and it is what a [mySites.guru subscription](#) is for.

---

## Further Reading

- [DJ-HelpfulArticles 1.3: Security Update](#) - the vendor advisory, with the FAQ on stored values and the list of what was tested.
- [DJ-HelpfulArticles product page](#) - the free Joomla extension this post is about, with the download.
- [CWE-79: Improper Neutralization of Input During Web Page Generation](#) - the weakness class the vendor assigned to this flaw.
- [OWASP Cross Site Scripting Prevention Cheat Sheet](#) - why output encoding is the defence, and why escaping for the database is not it.
- [X-Forwarded-For on MDN](#) - what the header is for, and why a client can write anything into it.

# Frequently Asked Questions

## What did DJ-HelpfulArticles 1.3 fix?

A stored cross-site scripting flaw in the article rating feature. The widget accepted a visitor IP address supplied by the browser, stored it without checking it was an IP address, and displayed it unescaped in the administrator's Helpful articles overview. In 1.3 the IP comes from the server connection, is validated, and stored IPs, article titles, feedback reasons and dates are escaped before they are rendered.

## Is there a CVE for the DJ-HelpfulArticles 1.3 fix?

Yes. The Joomla CNA published [CVE-2026-102800](#) on 27 October 2026, the day of the release, and scores it CVSS 4.0 8.7 High, crediting Ala Arfaoui. Our own assessment of the advisory is 8.6 High.

## Which DJ-HelpfulArticles versions are affected?

The [CVE-2026-102800](#) record lists 1.0.0 to 1.2.0 as affected. DJ-Extensions' advisory names 1.2. Versions 1.0.0 to 1.1.0 also have a separate, earlier XSS, [CVE-2024-27183](#). Every version below 1.3 has a known XSS, so update to 1.3.

## Does updating to DJ-HelpfulArticles 1.3 remove values an attacker already planted?

No. The vendor's FAQ is explicit that the update does not delete previously stored malicious values. Output escaping stops them running in the updated overview, but the records stay in the database until you remove them.

## Who found the DJ-HelpfulArticles flaw?

DJ-Extensions credits Ala Arfaoui. This is the vendor's fix. mySites.guru did not find or report it; we read the advisory and added the affected version to our vulnerability database the same day.

## Can mySites.guru show me which sites run a vulnerable DJ-HelpfulArticles?

Yes. The flaw was added to the mySites.guru vulnerability database on 27 October 2026, and widened to the CVE record's range when it was published, so any connected Joomla site running DJ-HelpfulArticles below 1.3 is flagged on its dashboard for [CVE-2026-102800](#). Sites on 1.1.0 and below are also flagged for [CVE-2024-27183](#).

**AI MODIFIED**

Written and edited by a human, with AI assistance. [Our approach to AI](#)

# Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.  
No credit card required.

<https://manage.mysites.guru/en/register>

## Get in touch

Phil E. Taylor  
[phil@phil-taylor.com](mailto:phil@phil-taylor.com)

mySites.guru

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

[mysites.guru](https://mysites.guru)