← View all Vulnerabilities

CVE-2025-31675

Cross-Site Scripting

Affects Link in Drupal 7

Versions >=7.1.0 <=7.1.12

Patch Available

This Vulnerability has been fixed in the Never-Ending Support (NES) version offered by HeroDevs.

View NES Solution →

Overview

Drupal is an open-source content management system known for its flexibility, robust features, and strong community support. Organizations of all sizes use it to build and manage dynamic websites and web applications. The Link module in Drupal core provides secure link construction to the system.

The exploit was also found in versions of the Link module used by Drupal 7.

The fix provided by HeroDevs introduces the `AttributeXss` class, which parses attribute strings into arrays while skipping prohibited attributes and selectively stripping dangerous protocols from URI-like values unless the attribute is safe (e.g., title, class, or data-*). The `sanitizeAttributes()` method processes attribute arrays by reconstructing and filtering each key-value pair, ensuring only safe ones are retained before rendering, thus preventing malicious attributes from reaching the output.

A cross-site scripting (XSS) vulnerability allows attackers to inject malicious scripts into webpages. It often occurs when a

Vulnerability Details

SEVERITY	Medium
ID	CVE-2025-31675
PROJECT AFFECTED	Link
VERSIONS AFFECTED	>=7.1.0 <=7.1.12
PUBLISHED DATE	February 2, 2026
≈ FIX DATE	March 18, 2025

site fails to properly validate or sanitize user input, enabling the execution of unauthorized code within a victim's browser. It is included in the OWASP Top Ten list of vulnerabilities, specifically in the third category of Injection. A web site compromised in this way may experience:

- Session hijacking
- Data theft
- Malware distribution
- Defacement or phishing, and
- Privilege escalation.

This issue affects all versions of Drupal 7 Link below 7.1.13 and is patched in Link NES version 7.1.14.

Details

Module Info

- **Product:** Drupal
- **Affected code:** `Link module`
- **Affected versions:** **<7.1.13**
- **Project page:** https://www.drupal.org/project/drupal
- **Fixed in:** Link NES 7.1.14

Vulnerability Info

This medium-severity vulnerability is found in all versions of the Link module lower than 7.13.

The exploit first described in Drupal 10 core (CVE-2025-31675) is a stored cross-site scripting (XSS) vulnerability affecting the Link field. Insufficient sanitization allows attackers with edit permissions—typically via web services, REST APIs, or custom/contrib modules—to inject malicious attributes into link render arrays. For instance, an attacker could add attributes like `onmouseover="alert('XSS')"` or `style="javascript:alert('XSS')",` which would be rendered in the HTML output. When a victim views or interacts with the link (e.g., hovering over it), the injected JavaScript executes in their browser context, potentially leading to session hijacking, data theft, or further attacks. This is mitigated if no link fields are

FIXED IN	NES for Drupal 7
CATEGORY	Cross-Site Scripting

used or if the Link module is disabled, and it requires attacker access to modify link attributes, making it moderately critical.

Steps To Reproduce

1. Install and enable a susceptible version of Link (any version under 7.1.13).

2. Install and enable the Services and Libraries modules.

3. Go to Structure › Services › Add and create a new endpoint:

- machine_name: api
- server: REST
- path to endpoint: api
- do not enable authentication

4. Make no changes to the field formatters.

5. Go to admin/structure/services/list/api/resources, click “Node” then click Save.

6. Verify the endpoint at http://‹your-site›/api. You should see: “Services Endpoint "api" has been set up successfully.”

7. Add a link field to the Article type: /admin/structure/types/manage/article/fields

8. Check Bypass Content Access Control for Node for the Anonymous user at admin/people/permissions/1.

9. Send a POST request to http://‹your-site›/api/node to create a node with a malicious `onmouseover` attribute in the Link field. Be sure to replace ‹your-site› below.

```
curl -X POST \
  -H "Content-Type: application/json" \
  -d '{
    "title": "XSS Test",
    "type": "article",
    "field_link": {
      "und": [{
        "url": "http://example.com",
        "title": "Click me",
        "attributes": {
          "onmouseover": "alert(\"XSS\")"
        }
      }]
    }
```

```
  }' \
  https://<your-site>/api/node
```

The result will be:

```
<result><nid>1</nid><uri>https://<your-site>/api/node
```

10. Visit the new node at /node/1 and hover over the link. Observe the dialog box appear.

Addressing The Issue

Users of the affected component(s) should address this exploit in one of the following ways:

- Ensure only trusted users have access to APIs or the database through which a malicious link can be added.
- Sign up for post-EOL security support; HeroDevs customers get immediate access to a patched version of this module.

Credits

- Samuel Mortenson (samuel.mortenson)

Additional Resources

- This exploit was first found in later versions of Drupal: Drupal core - Moderately critical - Cross Site Scripting - SA-CORE-2025-004
  https://www.drupal.org/SA-CORE-2025-004
- NIST CVE
  https://nvd.nist.gov/vuln/detail/CVE-2025-31675

Previous
CVE-2026-0748

Next
CVE-2026-1556

herodevs

Drop-in replacements for deprecated open source software that keeps you secure and compliant.

+1 877-586-1965
hello@herodevs.com
8850 S 700 E #2437
Sandy, UT 84070

Overview

All Products

Explore Pricing

Get a Custom Quote

NES Documentation

Never-Ending Support (NES) Products

Angular
AngularJS
Spring
.NET
Node.js
Struts
Bootstrap
Vue 2
PostgreSQL
Apache Grails
Apache Solr & Lucene
Apache Tapestry
Apache Tomcat
CometD
Django
Drupal 7
ESLint
Express
Fastify
Grunt
Hibernate
Jetty
jQuery
Knockout.js
Lodash
NestJS
Next.js
Nuxt

Solutions

Financial Services
Healthcare
Technology
Government
IT Security Managers
Software Development Managers
Engineers Leaders
Compliance-Focused Decision-Makers

Company

Home
Contact
About Us
We are Hiring!

Resources

Blog
Vulnerability Directory
Open Source Sustainability Fund
Shows
Case Studies
Webinars
EOL Dataset
Newsletters
White Papers
eBooks
Media Kit
What is EOL Security?

Partners

PHP

Protractor

Rails

Vuetify

HeroDevs Partner Program

Become a Reseller

Privacy Policy Terms of Service