



# Advanced iFrame <= 2024.1 - Authenticated (Contributor+) Stored Cross-Site Scripting

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

## Summary

<b>CVE</b>	CVE-2024-1341
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-02-29 05:15:09 UTC
<b>Updated</b>	2026-04-08 18:20:34 UTC
<b>Description</b>	The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's advanced_iframe s

## 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**

**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	security@wordfence.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	4.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N

## 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="#">Tinywebgallery</a>	<a href="#">Advanced Iframe</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Mdempfle</a>	<a href="#">Advanced IFrame</a>	affected 2024.1 semver	Not specified

### References

Reference	Source	Link
<a href="#">plugins.trac.wordpress.org/changeset</a>	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="#">plugins.t</a>
<a href="#">www.wordfence.com/threat-intel/vulnerabilities/id/699e5c80-8a11-4f67-8b17-41170...</a>	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="#">www.wo</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.</a>



### Vendor Comments And Credit

Discovery Credit  
**CNA: Fariq Fadillah Gusti Insani (en)**

### Additional Advisory Data

Source	Time	Event
CNA	2024-02-28T00:00:00.000Z	Disclosed

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

[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)