



Dino Game – Embed Google Chrome Dinosaur Game in WordPress <= 1.1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2024-11388
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-21 11:15:27 UTC
Updated	2026-04-08 19:19:38 UTC
Description	The Dino Game – Embed Google Chrome Dinosaur Game in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting (XSS) via the 'dino_game_embed' shortcode. An authenticated user with Contributor+ or higher privileges can inject malicious JavaScript code into the game embed, which is then served to all users viewing the page. This can lead to session hijacking, defacement, or other malicious actions depending on the injected code.

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

EPSS: 0.157310000 probability, percentile 0.947200000 (date 2026-04-13)

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	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/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	Tahmid-ul	Dino Game	All	All	All	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Tahmidulkarim	Dino Game Embed Google Chrome Dinosaur Game In Your Website	affected 1.1.0 semver	Not specified	

References		
Reference	Source	Link
plugins.trac.wordpress.org/browser/dino-game/trunk/dino-game.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/changeset/3193638/dino-game/trunk/dino-game.php	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/b1acc5f8-bd77-42e0-96d5-63603...	security@wordfence.com	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



Vendor Comments And Credit	
Discovery Credit	
CNA: SOPROBRO (en)	

Additional Advisory Data		
Source	Time	Event
CNA	2024-11-20T13:37:17.000Z	Disclosed

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

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report