



WordPress Simple Video Embedder plugin <= 2.2 - Auth. Stored Cross-Site Scripting (XSS) vulnerability

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

Summary

CVE	CVE-2022-44590
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-09 22:15:25 UTC
Updated	2026-04-28 19:18:54 UTC
Description	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in James Lao's Simple Video Embedder plugin <= 2.2 o

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 Cross-site Scripting (XSS)

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	audit@patchstack.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	CVSS	5.4	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	Simple Video Embedder Project	Simple Video Embedder	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	James Lao	Simple Video Embedder WordPress Plugin	affected <= 2.2 2.2 custom	Not specified

References

Reference	Source
Simple Video Embedder – WordPress plugin WordPress.org	af854a3a-2127-422b-
WordPress Simple Video Embedder plugin <= 2.2 - Auth. Stored Cross-Site Scripting (XSS) vulnerability - Patchstack	af854a3a-2127-422b-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Vulnerability discovered by thiennv (Patchstack Alliance) (en)

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

© CVE.report 2026 |

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](#)