



CVE-2022-25610

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

Summary

CVE	CVE-2022-25610
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-25 19:15:00 UTC
Updated	2022-12-02 19:29:00 UTC
Description	Unauthenticated Stored Cross-Site Scripting (XSS) in Simple Ajax Chat <= 20220115 allows an attacker to store the malicious

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Plugin-planet	Simple Ajax Chat	All	All	All	All
Application	Simpleajaxchat Project	Simple Ajax Chat	All	All	All	All

References

Reference	Source
WordPress Simple Ajax Chat plugin <= 20220115 - Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability - Patchstack	CONFIRM
Simple Ajax Chat – WordPress plugin WordPress.org	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Philippe Dourassov (Patchstack Alliance)

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](#)