



CVE-2021-36895

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

Summary

CVE	CVE-2021-36895
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-26 19:15:00 UTC
Updated	2022-05-03 20:04:00 UTC
Description	Unauthenticated Cross-Site Scripting (XSS) vulnerability in Tripetto's Tripetto plugin <= 5.1.4 on WordPress via SVG image

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tripetto	Tripetto	All	All	All	All

References

Reference	Source
WordPress Tripetto plugin <= 5.1.4 - Unauthenticated Cross-Site Scripting (XSS) vulnerability via SVG image upload - Patchstack	CONFIRM
WordPress form builder plugin for conversational forms – Tripetto – WordPress plugin WordPress.org	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Ngo Van Thien (Patchstack Alliance)

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

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