



CVE-2021-25978

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-25978
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-07 18:15:00 UTC
Updated	2021-11-09 18:21:00 UTC
Description	Apostrophe CMS versions between 2.63.0 to 3.3.1 are vulnerable to Stored XSS where an editor uploads an SVG file that c

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
sanitize SVG uploads, including previous uploads · apostrophecms/apostrophe@c8b94ee · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

Vendor Comments And Credit

Discovery Credit

LEGACY: Daniel Elkabes

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

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