BentoPDF: Stored XSS via Markdown Editor Leading to Persistent File Exfiltration

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41653
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 19:16:00 UTC
Updated	2026-05-07 19:51:36 UTC
Description	BentoPDF is a client-side PDF toolkit that is self hostable. Prior to version 2.8.3, a cross-site scripting vulnerability was iden

Risk And Classification

Primary CVSS: v4.0 7 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000470000 probability, percentile 0.145830000 (date 2026-05-12)

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
4.0	security-advisories@github.com	Secondary	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:L/VA:N/SC:N/S
4.0	CNA	DECLARED	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:L/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Active

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Alam00000	Bentopdf	affected < 2.8.3	Not specified

References

Reference	Source	Link	Tags
github.com/alam00000/bentopdf/security/advisories/GHSA-6vh8-4frx-647f	security-advisories@github.com	github.com	
github.com/alam00000/bentopdf/releases/tag/v2.8.3	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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