



WordPress Digital Lottery plugin <= 3.0.5 - Arbitrary File Upload vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2024-49242
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-16 14:15:09 UTC
Updated	2026-04-29 10:16:35 UTC
Description	Unrestricted Upload of File with Dangerous Type vulnerability in Shafiq Digital Lottery digital-lottery allows Upload a Web S

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from audit@patchstack.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

EPSS: 0.009700000 probability, percentile 0.766910000 (date 2026-05-05)

Problem Types: CWE-434 | CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Shafiq	Digital Lottery	affected 3.0.5 custom	Not specified
ADP	Shafiq	Digital Library	affected 3.0.5 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/digital-lottery/vulnerability/wordp...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy:

Vendor Comments And Credit

Discovery Credit

CNA: stealthcopter | Patchstack Bug Bounty Program (en)

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