



WordPress Designer plugin <= 1.4.1 - Local File Inclusion vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2024-54225
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-09 13:15:42 UTC
Updated	2026-04-23 15:21:56 UTC
Description	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in c

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from audit@patchstack.com

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

Problem Types: CWE-98 | CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector	Network
Attack Complexity	High
Privileges Required	Low
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Codegearthemes	Designer	affected 1.4.1 custom	Not specified
ADP	Codegearthemes	Designer	affected 1.3.3 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/designer/vulnerability/wordpress-de...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

Vendor Comments And Credit

Discovery Credit

CNA: João Pedro S Alcântara (Kinorth) | Patchstack Bug Bounty Program (en)

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