



WordPress Z-Downloads plugin <= 1.11.3 - Auth. Arbitrary File Upload vulnerability

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

Summary

CVE	CVE-2024-34555
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-14 15:39:21 UTC
Updated	2026-04-28 19:25:26 UTC
Description	Unrestricted Upload of File with Dangerous Type vulnerability in URBAN BASE Z-Downloads.This issue affects Z-Downloa

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: 0.079090000 probability, percentile 0.920450000 (date 2026-04-28)

Problem Types: CWE-434 | 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	9.1	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

Integrity

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	URBAN BASE	Z-Downloads	affected n/a 1.11.3 custom	Not specified
ADP	Urban Base	Z-downloads	affected 1.11.3 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/z-downloads/wordpress-z-downloads-plug...	af854a3a-2127-422b-91ae-364da2661108	patchstack
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

CNA: younsoung kim (Patchstack Alliance) (en)

CNA: SeoHyeon Lee (Patchstack Alliance) (en)

CNA: MyungJu Kim (Patchstack Alliance) (en)

CNA: SeoHee Kang (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 1.11.4 or a higher version.

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

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