WordPress Multiple Page Generator Plugin <= 3.4.0 - Auth. Remote Code Execution (RCE) vulnerability

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

Summary

CVE	CVE-2024-27951
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-03 12:15:11 UTC
Updated	2026-04-28 19:23:34 UTC
Description	Unrestricted Upload of File with Dangerous Type vulnerability in Themeisle Multiple Page Generator Plugin – MPG allows U

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from nvd@nist.gov

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

EPSS: 0.005250000 probability, percentile 0.670250000 (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	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/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:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Themeisle	Multiple Page Generator	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Themeisle	Multiple Page Generator Plugin MPG	affected n/a 3.4.0 custom	Not specified
ADP	Themeisle	Multiple Page Generator	affected 3.4.0 custom	Not specified

References

Reference	Source
WordPress Multiple Page Generator Plugin <= 3.4.0 - Remote Code Execution (RCE) vulnerability - Patchstack	af854a3a-2127-422b-91ae-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Majed Refaea (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 3.4.1 or a higher version.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report