WordPress Gallery Plugin – NextGEN Gallery <= 3.59 - Missing Authorization to Unauthenticated Information Disclosure

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

Summary

CVE	CVE-2024-3097
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-09 19:15:39 UTC
Updated	2026-04-08 18:21:19 UTC
Description	The WordPress Gallery Plugin – NextGEN Gallery plugin for WordPress is vulnerable to unauthorized access of data due to

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	security@wordfence.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagely	Nextgen Gallery	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Smub	Photo Gallery Sliders Proofing And Themes NextGEN Gallery	affected 3.59 semver	Not specified
ADP	Imagely	Nextgen Gallery	affected 3.59 semver	Not specified

References

Reference	Source
zpbrent.github.io/pocs/8-plugin-nextgen-gallery-InfoDis-20240327.mp4	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/browser/nextgen-gallery/trunk/src/REST/Admin/Block.php	af854a3a-2127-422b-91ae-364da2661108
www.wordfence.com/threat-intel/vulnerabilities/id/75f87f99-9f0d-46c2-a6f1-3c1ea...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/changeset/3063940/nextgen-gallery/trunk/src/REST/Admin/Block.php	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Peng Zhou (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-05T12:00:00.000Z	Disclosed

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