Ajax Load More <= 7.0.1 - Authenticated (Admin+) Directory Traversal to Arbitrary File Read

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

Summary

CVE	CVE-2024-1790
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-09 19:15:19 UTC
Updated	2026-04-08 18:20:49 UTC
Description	The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to Path Traversal in all versions up to, a

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from security@wordfence.com

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

Problem Types: CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
High

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Dcooney	Ajax Load More Infinite Scroll Load More Lazy Load	affected 7.0.1 semver	Not specified

References

Reference	Source	L
plugins.trac.wordpress.org/changeset/3056137/ajax-load-more/tags/7.1.0/core/functions.php	af854a3a-2127-422b-91ae-364da2661108	p
plugins.trac.wordpress.org/browser/ajax-load-more/trunk/admin/functions/layouts.php	af854a3a-2127-422b-91ae-364da2661108	p
plugins.trac.wordpress.org/changeset/3056137/ajax-load-more/tags/7.1.0/admin/functions/l...	af854a3a-2127-422b-91ae-364da2661108	p
www.wordfence.com/threat-intel/vulnerabilities/id/86090ab4-9f1d-4a92-a302-11852...	af854a3a-2127-422b-91ae-364da2661108	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

Vendor Comments And Credit

Discovery Credit

CNA: Hoa Le Ngoc (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-03-26T00:00:00.000Z	Disclosed

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