Salient Core <= 2.0.7 - Authenticated (Contributor+) Local File Inclusion via Shortcode

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

Summary

CVE	CVE-2024-3812
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-18 06:15:08 UTC
Updated	2026-04-08 19:21:27 UTC
Description	The Salient Core plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.0.7 via the

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security@wordfence.com

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

EPSS: 0.003400000 probability, percentile 0.568100000 (date 2026-04-12)

Problem Types: CWE-98 | 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	security@wordfence.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	DECLARED	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

ntegrity

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	ThemeNectar	Salient Core	affected 2.0.7 semver	Not specified
ADP	Themenectar	Salient Core	affected 2.0.7 semver	Not specified

References

Reference	Source	Link
themeforest.net/item/salient-responsive-multipurpose-theme/4363266	af854a3a-2127-422b-91ae-364da2661108	themefor
www.wordfence.com/threat-intel/vulnerabilities/id/ebd3b70e-a06a-4dcc-a6af-dbe64...	af854a3a-2127-422b-91ae-364da2661108	www.wo
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-15T00:00:00.000Z	Discovered
CNA	2024-04-15T00:00:00.000Z	Vendor Notified
CNA	2024-04-17T00:00:00.000Z	Disclosed

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**