FULL <= 3.1.12 - Unauthenticated Stored Cross-Site Scripting via License Plan Parameter

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

Summary

CVE	CVE-2024-6447
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-11 00:15:02 UTC
Updated	2026-04-08 17:19:11 UTC
Description	The FULL – Cliente plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the license plan parameter in all v

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from security@wordfence.com

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

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Changed

Confidentiality
Low

Integrity

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fullservices	FULL Cliente	affected 3.1.12 semver	Not specified

References

Reference	Source	Li
plugins.trac.wordpress.org/browser/full-customer/tags/3.1.12/app/controller/inc/License.php	af854a3a-2127-422b-91ae-364da2661108	plu
www.wordfence.com/threat-intel/vulnerabilities/id/2f3ad1e0-1ae3-44cd-aa2a-dbb3a...	af854a3a-2127-422b-91ae-364da2661108	ww
plugins.trac.wordpress.org/browser/full-customer/tags/3.1.12/app/controller/actions.php	af854a3a-2127-422b-91ae-364da2661108	plu
plugins.trac.wordpress.org/browser/full-customer/tags/3.1.12/app/api/Connection.php	af854a3a-2127-422b-91ae-364da2661108	plu
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

CNA: Matthew Rollings (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-06-21T00:00:00.000Z	Discovered
CNA	2024-07-10T11:26:16.000Z	Disclosed

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

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