



WordPress FW Food Menu plugin <= 6.0.0 - Arbitrary File Deletion Vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2025-49448
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-27 12:15:38 UTC
Updated	2026-04-23 15:31:42 UTC
Description	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Fastw3b LLC FW Food Menu

Risk And Classification

Primary CVSS: v3.1 8.6 HIGH from audit@patchstack.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
3.1	CNA	CVSS	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity	

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Fastw3b LLC	FW Food Menu	affected 6.0.0 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/fw-food-menu/vulnerability/wordpress...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, au

Vendor Comments And Credit

Discovery Credit

CNA: LVT-tholv2k | Patchstack Bug Bounty Program (en)

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