WordPress Blossom Shop theme <= 1.1.7 - Cross Site Request Forgery (CSRF) vulnerability

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

Summary

CVE	CVE-2024-37412
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-02 12:15:18 UTC
Updated	2026-04-01 16:17:23 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in blossomthemes Blossom Shop blossom-shop allows Cross Site Reque

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-352 | CWE-352 Cross-Site Request Forgery (CSRF)

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Blossomthemes	Blossom Shop	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Blossomthemes	Blossom Shop	affected 1.1.7 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Theme/blossom-shop/vulnerability/wordpress...	audit@patchstack.com	patchstack.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: Dhabaleshwar Das | Patchstack Bug Bounty Program (en)

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