WordPress CartBounty plugin <= 8.2 - Cross Site Request Forgery (CSRF) vulnerability

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

Summary

CVE	CVE-2024-47634
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-20 11:15:02 UTC
Updated	2026-04-01 16:18:18 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in Streamline CartBounty – Save and recover abandoned carts for WooC

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/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
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Majas-lapu-izstrade	Cartbounty	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Streamline	CartBounty Save And Recover Abandoned Carts For WooCommerce	affected 8.2 custom	Not specified
ADP	Woocommerce	Streamline.lv	affected 8.2 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/woo-save-abandoned-carts/vulnerabil...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: Mika | Patchstack Bug Bounty Program (en)

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