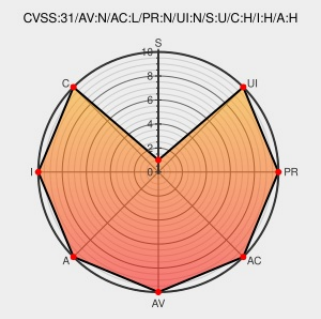
CVE-2021-27817

Published on: 03/15/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:48 PM UTC

CVE-2021-27817

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Shopxo from Shopxo contain the following vulnerability:

A remote command execution vulnerability in shopxo 1.9.3 allows an attacker to upload malicious code generated by phar where the suffix is JPG, which is uploaded after modifying the phar suffix.

CVE-2021-27817 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Page not found · GitHub · GitHub	Broken Link, github.com, text/html, Inactive Link, Not Archived	MISC github.com/h4ckdepy/vuls/blob/main/shopxo.md

GitHub - gongfuxiang/shopxo: ShopXO免费开源商城系统、国内领先企业级B2C免费开源电商系统，包含PC、h5、微信小程序、支付宝小程序、百度小程序、头条&抖音小程序、QQ小程序，遵循MIT开源协议发布、基于 ThinkPHP5.1框架研发

Product
github.com
text/html

MISC github.com/gongfuxiang/shopxo

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Shopxo	Shopxo	1.9.3	All	All	All

cpe:2.3:a:shopxo:shopxo:1.9.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→