



jackq XCMS Backend

ProductImageController.class.php upload unrestricted upload

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2025-15110
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-27 20:15:41 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability has been found in jackq XCMS up to 3fab5342cc509945a7ce1b8ec39d19f701b89261. Affected is the function <code>uploadImage</code> in <code>ProductImageController.class.php</code> . The vulnerability allows a remote attacker to upload arbitrary files to the server. The attack is performed by sending a specially crafted request to the <code>uploadImage</code> endpoint. The request contains a <code>file</code> parameter with a value that is a valid image file name, followed by a double slash and a backslash, and then the name of the file to be uploaded. For example, <code>file=image.jpg//%00../../../../../../var/www/html/uploads/image.jpg</code> . The server will then upload the file to the specified location. The vulnerability is caused by the fact that the server does not properly sanitize the <code>file</code> parameter. It only checks for the presence of a valid image file name, but it does not check for the presence of a valid file path. This allows an attacker to bypass the file upload restrictions and upload arbitrary files to the server.

Risk And Classification

Primary CVSS: v4.0 2 LOW from cna@vulldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-284 | CWE-434 | CWE-434 Unrestricted Upload | CWE-284 Improper Access Controls

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vulldb.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	4.7	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vulldb.com	Secondary	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P
2.0	CNA	DECLARED	5.8		AV:N/AC:L/Au:M/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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



CVSS v3.1 Breakdown

CVSS V3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Jackq	Xcms	1.1	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Jackq	XCMS	affected 3fab5342cc509945a7ce1b8ec39d19f701b89261	Not specified

References			
Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
gitee.com/jackq/XCMS	cna@vuldb.com	gitee.com	
gitee.com/jackq/XCMS/issues/IDC5C8	134c704f-9b21-4f2e-91b3-4a467353bcc0	gitee.com	Exploit, Issue Tracking, Third Party Advis
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Required, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: 3fab5342cc509945a7ce1b8ec39d19f701b89261

CNA: tormanager (VulDB User) (en)

Additional Advisory Data		
Source	Time	Event
CNA	2025-12-26T01:00:00.000Z	VulDB entry created
CNA	2025-12-27T00:00:00.000Z	Advisory disclosed
CNA	2026-01-09T22:16:50.000Z	VulDB entry last update
There are currently no legacy QID mappings associated with this CVE.		

© [CVE.report](#) 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)