

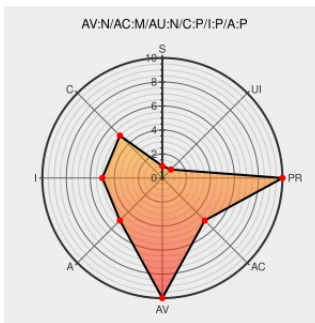


CVE-2011-4106

Published on: 10/26/2013 12:00:00 AM UTC

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

CVE-2011-4106

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Timthumb](#) from [Binarymoon](#) contain the following vulnerability:

TimThumb (timthumb.php) before 2.0 does not validate the entire source with the domain white list, which allows remote attackers to upload and execute arbitrary code via a URL containing a white-listed domain in the src parameter, then accessing it via a direct request to the file in the cache directory, as exploited in the wild in August 2011.

CVE-2011-4106 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
oss-security - Re: CVE request: wordpress plugin timthumb before 2.0 remote code execution	www.openwall.com text/html	MLIST [oss-security] 20111103 Re: CVE request: wordpress plugin timthumb before 2.0 remote code execution
Zero Day Vulnerability in many Wordpress Themes mm	web.archive.org text/html Inactive Link Not Archived	MISC markmaunder.com/2011/08/01/zero-day-vulnerability-in-many-wordpress-themes/
WordPress TimThumb Plugin - Remote Code Execution	Exploit www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 17602
TimThumb 2.0	www.binarymoon.co.uk text/html	CONFIRM www.binarymoon.co.uk/2011/08/timthumb-

Issue 212 - timthumb - Zero day vulnerability that gives remote attacker shell access - image crop zoom resize management - Google Project Hosting

[Exploit](#)
[Patch](#)
[code.google.com](#)
[text/html](#)

 **CONFIRM**
code.google.com/p/timthumb/issues/detail?id=212

Multiple Wordpress Plugin timthumb.php Vulnerabilites

[Exploit](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

 **EXPLOIT-DB 17872**

Technical details and scripts of the Wordpress Timthumb.php hack | mm

[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#)
[Not Archived](#)

 **MISC**
markmaunder.com/2011/08/02/technical-details-and-scripts-of-the-wordpress-timthumb-php-hack/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Binarymoon	Timthumb	All	All	All	All
cpe:2.3:a:binarymoon:timthumb:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/cybersecurity	KashmirBlack botnet behind attacks on CMSs like WordPress, Joomla, Drupal, others (16 vulnerabilities exploited)	2020-10-26 09:38:41

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

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