



CVE-2014-4663

Published on: 07/15/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-4663

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

TimThumb 2.8.13 and WordThumb 1.07, when Webshot (aka Webshots) is enabled, allows remote attackers to execute arbitrary commands via shell metacharacters in the src parameter.

CVE-2014-4663 has been assigned by [M](#) cve@mitre.org 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

Full Disclosure: Re: Wordpress TimThumb 2.8.13 WebShot Remote Code Execution (0-day)

[seclists.org](#)
[text/html](#)

[FULLDISC 20140701 Re: Wordpress TimThumb 2.8.13 WebShot Remote Code Execution \(0-day\)](#)

Full Disclosure: Wordpress TimThumb 2.8.13 WebShot Remote Code Execution (0-day)

[seclists.org](#)
[text/html](#)

[FULLDISC 20140624 Wordpress TimThumb 2.8.13 WebShot Remote Code Execution \(0-day\)](#)

About Secunia Research | Flexera

[secunia.com](#)
[Deprecated Link](#)
[text/plain](#)

[SECUNIA 59558](#)

Issue 485 - timthumb - Remote Code Execution - image crop zoom resize management - Google Project Hosting

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

[CONFIRM](#)
[code.google.com/p/timthumb/issues/detail?id=485](#)

Wordpress TimThumb 2.8.13 WebShot - Remote Code Execution (0day)

[Exploit](#)
[www.exploit-db.com](#)

[EXPLOIT-DB 33851](#)

Proof of Concept
text/html

TimThumb 2.8.13 Remote Code Execution ≈ Packet Storm

packetstormsecurity.com
text/html

 MISC
packetstormsecurity.com/files/127192/TimThumb-2.8.13-Remote-Code-Execution.html

r219 - timthumb - image crop zoom resize management - Google Project Hosting

code.google.com
text/html

 CONFIRM
code.google.com/p/timthumb/source/detail?r=219

oss-sec: Re: CVE request: timthumb remote code execution

seclists.org
text/html

 MLIST [oss-security] 20140627 Re: CVE request: timthumb remote code execution

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	2.8.13	All	All	All
Application	Binarymoon	Timthumb	2.8.13	All	All	All
Application	Binarymoon	Wordthumb	1.07	All	All	All
Application	Binarymoon	Wordthumb	1.07	All	All	All

cpe:2.3:a:binarymoon:timthumb:2.8.13:*:*:*:*:*:

cpe:2.3:a:binarymoon:timthumb:2.8.13:*:*:*:*:*:

cpe:2.3:a:binarymoon:wordthumb:1.07:*:*:*:*:*:

cpe:2.3:a:binarymoon:wordthumb:1.07:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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](#)