



# CVE-2011-4825

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2011-4825
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-12-15 03:57:34 UTC
<b>Updated</b>	2026-04-29 01:13:23 UTC
<b>Description</b>	Static code injection vulnerability in inc/function.base.php in Ajax File and Image Manager before 1.1, as used in tiny mce be

## Risk And Classification

**Primary CVSS:** v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

**Problem Types:** CWE-94 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpletter	Ajax File And Image Manager	0.5	All	All	All

Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.5.5	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.5.7	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.6	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.6.12	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.7.10	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.7.8	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.8	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.8.24	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.8.8	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.8.9	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	0.9	All	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	1.0	beta1	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	1.0	beta2	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	1.0	rc1	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	1.0	rc2	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	1.0	rc3	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	1.0	rc4	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	1.0	rc5	All	All
Application	<a href="#">Phpletter</a>	<a href="#">Ajax File And Image Manager</a>	All	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.0	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.1	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.10	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.11	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.12	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.13	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.14	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.15	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.16	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.17	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.18	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.2	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.3	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.4	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.5	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.6	All	All	All
Application	<a href="#">Phpmymfaq</a>	<a href="#">Phpmymfaq</a>	2.6.7	All	All	All

Application	<a href="#">Phpmyfaq</a>	<a href="#">Phpmyfaq</a>	2.6.8	All	All	All
Application	<a href="#">Phpmyfaq</a>	<a href="#">Phpmyfaq</a>	2.6.9	All	All	All
Application	<a href="#">Phpmyfaq</a>	<a href="#">Phpmyfaq</a>	2.7.0	All	All	All
Application	<a href="#">Tinymce</a>	<a href="#">Tinymce</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

#### References

Reference	Source	Link
#2005 (Remote Code Execution Vulnerability) – zenphoto	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.zenphoto.org</a>
Ajax File and Image Manager 'data.php' PHP Code Injection Vulnerability	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.secureworks.com</a>
Ajax File and Image Manager v1.0 Final Remote Code Execution Vulnerability	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.exploit-db.com</a>
phpMyFAQ homepage - open source FAQ software   Security Advisory 2011-09-28	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.phpmyfaq.com</a>
DOWNLOAD	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.phpmyfaq.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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](#)