



# CVE-2016-4862

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2016-4862
<b>State</b>	PUBLISHED
<b>Assigner</b>	jpccert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-20 18:59:00 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	Twigmo bundled with CS-Cart 4.3.9 and earlier and Twigmo bundled with CS-Cart Multi-Vendor 4.3.9 and earlier allow rem

## Risk And Classification

**Primary CVSS:** v3.0 8.8 HIGH from nvd@nist.gov

**CVSS:**3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Problem Types:** CWE-20 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cs-cart	Cs-cart	All	All	All	All
Application	Cs-cart	Cs-cart	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
CS-Cart add-on 'Twigmo' CVE-2016-4862 PHP Object Injection Vulnerability	af854a3
JVNDB-2016-000157 - JVN iPedia	af854a3
JVN#55389065: CS-Cart add-on "Twigmo" vulnerable to PHP object injection	af854a3
セキュリティ :: 【CVE-2016-4862】 TwigmoアドオンにおけるPHPオブジェクトインジェクションの脆弱性について - ブログ記事	af854a3
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

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](#)