



CVE-2006-0755

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

Summary

CVE	CVE-2006-0755
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-18 02:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple PHP remote file include vulnerabilities in dotProject 2.0.1 and earlier, when register_globals is enabled, allow remo

Risk And Classification

Primary CVSS: v3.1 5.6 MEDIUM from ADP

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

EPSS: 0.112320000 probability, percentile 0.935270000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
2.0	nvd@nist.gov	Primary	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dotproject	Dotproject	2.0	All	All	All
Application	Dotproject	Dotproject	2.0.1	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
www.osvdb.org/23218	af854a3a-2127-422b-91ae-364da2661108	www
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23213	af854a3a-2127-422b-91ae-364da2661108	www
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exch
www.osvdb.org/23211	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23215	af854a3a-2127-422b-91ae-364da2661108	www
Secunia - Advisories - dotProject File Inclusion and Information Disclosure Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	secu

SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23217	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23216	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23209	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23214	af854a3a-2127-422b-91ae-364da2661108	www
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23210	af854a3a-2127-422b-91ae-364da2661108	www
Dotproject Multiple Remote File Include Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23212	af854a3a-2127-422b-91ae-364da2661108	www
www.osvdb.org/23219	af854a3a-2127-422b-91ae-364da2661108	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

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