



CVE-2016-6523

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2016-6523 |
| State | PUBLISHED |
| Assigner | mitre |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-12-09 20:59:03 UTC |
| Updated | 2026-05-06 22:30:45 UTC |
| Description | Multiple cross-site scripting (XSS) vulnerabilities in the media manager in Dotclear before 2.10 allow remote attackers to inj |

Risk And Classification

Primary CVSS: v3.0 6.1 MEDIUM from nvd@nist.gov

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

EPSS: 0.007930000 probability, percentile 0.740200000 (date 2026-05-10)

Problem Types: CWE-79 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------|---------|-------|----------|--|
| 3.0 | nvd@nist.gov | Primary | 6.1 | MEDIUM | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N |
| 2.0 | nvd@nist.gov | Primary | 4.3 | | AV:N/AC:M/Au:N/C:N/I:P/A:N |

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability
None
 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v2.0 Breakdown

Access Vector
Network

Access Complexity
Medium

Authentication
None

Confidentiality
None

Integrity
Partial

Availability
None
 AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------|----------|---------|--------|---------|----------|
| Application | Dotclear | Dotclear | 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 |
|--|--------------------------------------|--|
| oss-security - CVE request: XSS vulns in Dotclear v2.9.1 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com |
| oss-security - Re: CVE request: XSS vulns in Dotclear v2.9.1 | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com |
| Dotclear: CHANGELOG@18dc878c1178 | af854a3a-2127-422b-91ae-364da2661108 | hg.dotclear.org |
| Dotclear: changeset 3295:40d0207e520d | af854a3a-2127-422b-91ae-364da2661108 | hg.dotclear.org |
| Dotclear CVE-2016-6523 Multiple Cross Site Scripting Vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 | www.securityfocus.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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](#)