



CVE-2016-8905

Published on: 11/14/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:08 PM UTC

CVE-2016-8905

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

SQL injection vulnerability in the JSONTags servlet in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the sort parameter.

CVE-2016-8905 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
card-571-call-sort-method by erickgonzalez · Pull Request #8468 · dotCMS/core · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/dotCMS/core/pull/8468/

 BID 94311

text/html

text/html

[E MISC security.elarlang.eu/multiple-sql-injection-vulnerabilities-in-dotcms-8x-cve-full-disclosure.html](https://security.elarlang.eu/multiple-sql-injection-vulnerabilities-in-dotcms-8x-cve-full-disclosure.html)

text/html

 MISC github.com/dotCMS/core/pull/8460/

text/html

 [MISC seclists.org/fulldisclosure/2016/Nov/0](https://misc.seclists.org/fulldisclosure/2016/Nov/0)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	Dotcms	Dotcms	All	All	All	All
cpe:2.3:a:dotcms:dotcms:*:*:*:*:*.*						

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