



orderby parameter -> Links pages -> Screen in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the orderby parameter." />

CVE-2016-8906

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

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

CVE-2016-8906

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



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

SQL injection vulnerability in the "Site Browser > Links pages" screen in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the orderby parameter.

CVE-2016-8906 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	Patch	MISC github.com/dotCMS/core/pull/8468/

#8468 · dotCMS/core · GitHub	Vendor Advisory github.com text/html	
dotCMS Multiple SQL Injection Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 94311
Multiple SQL injection vulnerabilities in dotCMS (8x CVE Full Disclosure) - Security Elar Lang	Exploit Third Party Advisory security.elarlang.eu text/html	MISC security.elarlang.eu/multiple-sql-injection-vulnerabilities-in-dotcms-8x-cve-full-disclosure.html
Card 571 sql injection by dsilvam · Pull Request #8460 · dotCMS/core · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/dotCMS/core/pull/8460/
Full Disclosure: Multiple SQL injection vulnerabilities in dotCMS (8x CVE)	Exploit Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2016/Nov/0

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to 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