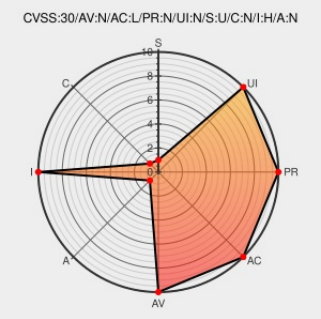
CVE-2016-8600

Published on: 10/28/2016 12:00:00 AM UTC

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

CVE-2016-8600

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dotcms from Dotcms contain the following vulnerability:

In dotCMS 3.2.1, attacker can load captcha once, fill it with correct value and then this correct value is ok for forms with captcha check later.

CVE-2016-8600 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2016-8600 dotCMS - CAPTCHA bypass by reusing valid code - Security | Elar Lang	Exploit, Third Party Advisory, security.elarlang.eu, text/html	MISC security.elarlang.eu/cve-2016-8600-dotcms-captcha-bypass-by-reusing-valid-code.html

Captcha can be programmatically reused by passing session id · Issue #9330 · dotCMS/core · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/dotCMS/core/issues/9330
dotCMS CVE-2016-8600 Security Bypass Vulnerability	cve.report (archive) text/html	BID 93798
Full Disclosure: CVE-2016-8600 dotCMS - CAPTCHA bypass by reusing valid code	Exploit Third Party Advisory VDB Entry seclists.org text/html	MISC seclists.org/fulldisclosure/2016/Oct/63

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	3.2.1	All	All	All
Application	Dotcms	Dotcms	3.2.1	All	All	All

cpe:2.3:a:dotcms:dotcms:3.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:dotcms:dotcms:3.2.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→