

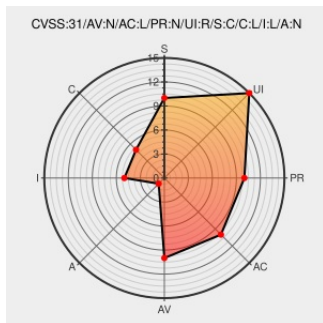


CVE-2011-3183

Published on: 01/14/2020 12:00:00 AM UTC

Last Modified on: 07/15/2021 08:42:00 PM UTC

CVE-2011-3183

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

Certain versions of [Concrete Cms](#) from [Concretecms](#) contain the following vulnerability:

A Cross-Site Scripting (XSS) vulnerability exists in the rcID parameter in Concrete CMS 5.4.1.1 and earlier.

CVE-2011-3183 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Concrete CMS - Concrete CMS** version **through 5.4.1.1**

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - Re: CVE Request: Concrete CMS 5.4.1.1 <= Cross Site Scripting	Exploit Mailing List Third Party Advisory	MISC www.openwall.com/lists/oss-security/2011/08/22/11

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	Concretecms	Concrete Cms	All	All	All	All
Application	Portlandlabs	Concrete Cms	All	All	All	All
cpe:2.3:a:concretecms:concrete_cms:*.*.*.*.*.*.*.*.						
cpe:2.3:a:portlandlabs:concrete_cms:*.*.*.*.*.*.*.*.						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→