



CVE-2013-5091

Published on: 10/04/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:36 PM UTC

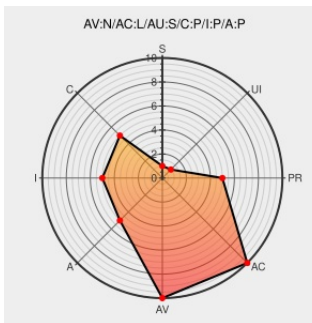
CVE-2013-5091

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

SQL injection vulnerability in CalendarCommon.php in vTiger CRM 5.4.0 and possibly earlier allows remote authenticated users to execute arbitrary SQL commands via the onlyforuser parameter in an index action to index.php. NOTE: this issue might be a duplicate of CVE-2011-4559.

CVE-2013-5091 has been assigned by [M](#) cve@mitre.org to track the vulnerability

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
No Description Provided	Broken Link osvdb.org Inactive Link Not Archived	OSVDB 76138
Vtiger CRM 5.4.0 (index.php, onlyforuser param) - SQL Injection	Exploit Third Party Advisory www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 28409
Vtiger CRM - Browse /vtiger CRM 5.4.0/Core Product at SourceForge.net	Patch Third Party Advisory sourceforge.net text/html	CONFIRM sourceforge.net/projects/vtigercrm/files/vtiger%20CRM%205.4.0/Core%20Product/

File Not Found

Third Party Advisory

www.htbridge.com

text/html

Inactive Link

Not Archived

MISC www.htbridge.com/advisory/HTB23168

NEOHAPSIS - Peace of
Mind Through Integrity
and Insight

Third Party Advisory

web.archive.org

text/html

Inactive Link

Not Archived

BUGTRAQ 20130918 SQL Injection in vtiger CRM

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	Vtiger	Vtiger Crm	1.0	All	All	All
Application	Vtiger	Vtiger Crm	2.0	All	All	All
Application	Vtiger	Vtiger Crm	2.0.1	All	All	All
Application	Vtiger	Vtiger Crm	2.1	All	All	All
Application	Vtiger	Vtiger Crm	3.0	All	All	All
Application	Vtiger	Vtiger Crm	3.0	beta	All	All
Application	Vtiger	Vtiger Crm	3.2	All	All	All
Application	Vtiger	Vtiger Crm	4	All	All	All
Application	Vtiger	Vtiger Crm	4	beta	All	All
Application	Vtiger	Vtiger Crm	4	beta	All	it
Application	Vtiger	Vtiger Crm	4	rc1	All	All
Application	Vtiger	Vtiger Crm	4.0	All	All	All
Application	Vtiger	Vtiger Crm	4.0.1	All	All	All
Application	Vtiger	Vtiger Crm	4.2	All	All	All
Application	Vtiger	Vtiger Crm	4.2	All	All	All
Application	Vtiger	Vtiger Crm	4.2	patch1	All	All
Application	Vtiger	Vtiger Crm	4.2.4	All	All	All
Application	Vtiger	Vtiger Crm	5.0.0	All	All	All
Application	Vtiger	Vtiger Crm	5.0.2	All	All	All
Application	Vtiger	Vtiger Crm	5.0.3	All	All	All
Application	Vtiger	Vtiger Crm	5.0.4	All	All	All
Application	Vtiger	Vtiger Crm	5.0.4	rc	All	All

Application	Vtiger	Vtiger Crm	5.1.0	All	All	All
Application	Vtiger	Vtiger Crm	5.1.0	rc	All	All
Application	Vtiger	Vtiger Crm	5.2.0	All	All	All
Application	Vtiger	Vtiger Crm	5.2.1	All	All	All
Application	Vtiger	Vtiger Crm	5.3.0	All	All	All
Application	Vtiger	Vtiger Crm	1.0	All	All	All
Application	Vtiger	Vtiger Crm	2.0	All	All	All
Application	Vtiger	Vtiger Crm	2.0.1	All	All	All
Application	Vtiger	Vtiger Crm	2.1	All	All	All
Application	Vtiger	Vtiger Crm	3.0	All	All	All
Application	Vtiger	Vtiger Crm	3.0	beta	All	All
Application	Vtiger	Vtiger Crm	3.2	All	All	All
Application	Vtiger	Vtiger Crm	4	All	All	All
Application	Vtiger	Vtiger Crm	4	beta	All	All
Application	Vtiger	Vtiger Crm	4	beta	All	it
Application	Vtiger	Vtiger Crm	4	rc1	All	All
Application	Vtiger	Vtiger Crm	4.0	All	All	All
Application	Vtiger	Vtiger Crm	4.0.1	All	All	All
Application	Vtiger	Vtiger Crm	4.2	All	All	All
Application	Vtiger	Vtiger Crm	4.2	All	All	All
Application	Vtiger	Vtiger Crm	4.2	patch1	All	All
Application	Vtiger	Vtiger Crm	4.2.4	All	All	All
Application	Vtiger	Vtiger Crm	5.0.0	All	All	All
Application	Vtiger	Vtiger Crm	5.0.2	All	All	All
Application	Vtiger	Vtiger Crm	5.0.3	All	All	All
Application	Vtiger	Vtiger Crm	5.0.4	All	All	All
Application	Vtiger	Vtiger Crm	5.0.4	rc	All	All
Application	Vtiger	Vtiger Crm	5.1.0	All	All	All
Application	Vtiger	Vtiger Crm	5.1.0	rc	All	All
Application	Vtiger	Vtiger Crm	5.2.0	All	All	All
Application	Vtiger	Vtiger Crm	5.2.1	All	All	All
Application	Vtiger	Vtiger Crm	5.3.0	All	All	All
Application	Vtiger	Vtiger Crm	All	All	All	All
cpe:2.3:a:vtiger:vtiger_crm:1.0:*****:						
cpe:2.3:a:vtiger:vtiger_crm:2.0:*****:						

cpe:2.3:a:vtiger:vtiger_crm:2.0.1:*****:
cpe:2.3:a:vtiger:vtiger_crm:2.1:*****:
cpe:2.3:a:vtiger:vtiger_crm:3.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:3.0:beta:*****:
cpe:2.3:a:vtiger:vtiger_crm:3.2:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:beta:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:beta:*.it:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:rc1:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.0.1:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.2:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.2:***:validation:***:
cpe:2.3:a:vtiger:vtiger_crm:4.2:patch1:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.2.4:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.2:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.3:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.4:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.4:rc:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.1.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.1.0:rc:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.2.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.2.1:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.3.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:1.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:2.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:2.0.1:*****:

cpe:2.3:a:vtiger:vtiger_crm:2.1:*****:
cpe:2.3:a:vtiger:vtiger_crm:3.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:3.0:beta:*****:
cpe:2.3:a:vtiger:vtiger_crm:3.2:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:beta:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:beta:.it:*****:
cpe:2.3:a:vtiger:vtiger_crm:4:rc1:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.0.1:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.2:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.2:***.validation:***:
cpe:2.3:a:vtiger:vtiger_crm:4.2:patch1:*****:
cpe:2.3:a:vtiger:vtiger_crm:4.2.4:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.2:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.3:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.4:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.0.4:rc:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.1.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.1.0:rc:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.2.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.2.1:*****:
cpe:2.3:a:vtiger:vtiger_crm:5.3.0:*****:
cpe:2.3:a:vtiger:vtiger_crm:*****:

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](#)