



CVE-2005-3820

Published on: 11/25/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

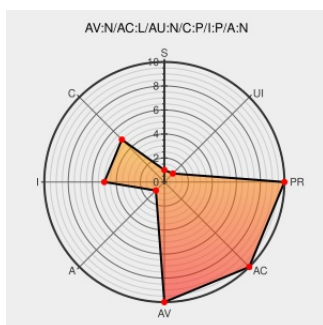
CVE-2005-3820

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Multiple directory traversal vulnerabilities in index.php in vTiger CRM 4.2 and earlier allow remote attackers to read or include arbitrary files, an ultimately execute arbitrary PHP code, via .. (dot dot) and null byte ("%00") sequences in the (1) module parameter and (2) action parameter in the Leads module, as also demonstrated by injecting PHP code into log messages and accessing the log file.

CVE-2005-3820 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.vupen.com
text/html

[VUPEN ADV-2005-2569](#)

VTiger CRM Multiple Input Validation Vulnerabilities

[cve.report \(archive\)](#)
text/html

[BID 15569](#)

Hardened-PHP Project - PHP Security - Advisory 23/2005

Vendor Advisory
www.hardened-php.net
text/html

[MISC www.hardened-php.net/advisory_232005.105.html](#)

SecurityTracker.com Archives - vtiger Multiple Input Validation Bugs Let Remote Users Conduct Cross-Site Scripting and SQL Injection Attacks and Execute Arbitrary Code

[securitytracker.com](#)
text/html

[SECTrack 1015271](#)

'[Full-disclosure] SEC Consult SA-20051125-0 :: More Vulnerabilities' - MARC	marc.info text/html	 FULLDISC 20051125 SEC Consult SA-20051125-0 :: More Vulnerabilities in vTiger CRM
Secunia - Advisories - vtiger CRM Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	 SECUNIA 17693
SecurityTracker.com Archives - vtiger Multiple Input Validation Bugs Let Remote Users Traverse the Directory, Conduct Cross-Site Scripting and SQL Injection Attacks, and Execute Arbitrary Code	securitytracker.com text/html	 SECTrack 1015274
VTiger CRM Multiple Input Validation Vulnerabilities	Exploit cve.report (archive) text/html	 BID 15562
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20051124 Advisory 23/2005: vTiger multiple vulnerabilities
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20051125 SEC Consult SA-20051125-0 :: More Vulnerabilities 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	All	All	All	All
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