PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

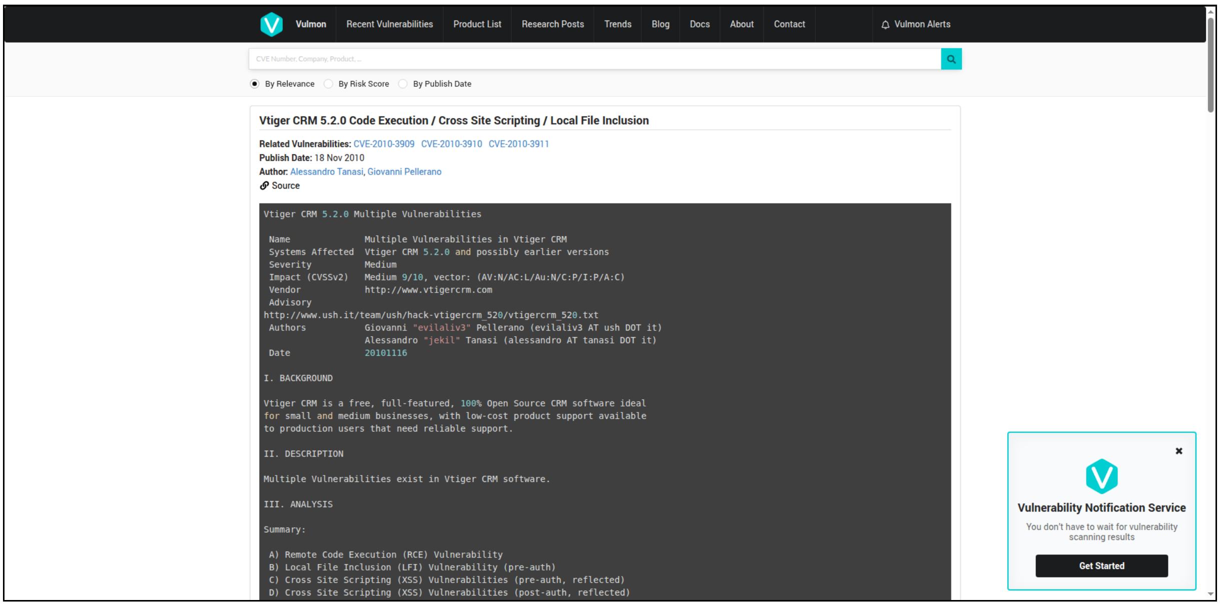
Source URL: https://vulmon.com/exploitdetails?qidtp=packetstorm_exploits&qid=d1a70a8595ea8ca876ebd07119717229

Archived Date: August 15, 2025 at 15:29

Document Type: Web Page Archive

Wayback Machine: https://web.archive.org/web/*/https://vulmon.com/exploitdetails?qidtp=packetstorm_exploits&qid=d1a70a8595ea8ca876ebd07119717229

Page Screenshot


Vulmon
Recent Vulnerabilities
Product List
Research Posts
Trends
Blog
Docs
About
Contact
Vulmon Alerts
CVE Number, Company, Product, ...
● By Relevance ○ By Risk Score ○ By Publish Date
Vulnerability Notification Service
You don't have to wait for vulnerability scanning results
Get Started

Vtiger CRM 5.2.0 Code Execution / Cross Site Scripting / Local File Inclusion

Related Vulnerabilities: CVE-2010-3909 CVE-2010-3910 CVE-2010-3911
Publish Date: 18 Nov 2010
Author: Alessandro Tanasi, Giovanni Pellerano
Source

```
Vtiger CRM 5.2.0 Multiple Vulnerabilities

 Name              Multiple Vulnerabilities in Vtiger CRM
 Systems Affected  Vtiger CRM 5.2.0 and possibly earlier versions
 Severity          Medium
 Impact (CVSSv2)   Medium 9/10, vector: (AV:N/AC:L/Au:N/C:P/I:P/A:C)
 Vendor            http://www.vtigercrm.com
 Advisory
http://www.ush.it/team/ush/hack-vtigercrm_520/vtigercrm_520.txt
 Authors           Giovanni "evilaliv3" Pellerano (evilaliv3 AT ush DOT it)
                   Alessandro "jekil" Tanasi (alessandro AT tanasi DOT it)
 Date              20101116

I. BACKGROUND

Vtiger CRM is a free, full-featured, 100% Open Source CRM software ideal
for small and medium businesses, with low-cost product support available
to production users that need reliable support.

II. DESCRIPTION

Multiple Vulnerabilities exist in Vtiger CRM software.

III. ANALYSIS

Summary:

 A) Remote Code Execution (RCE) Vulnerability
 B) Local File Inclusion (LFI) Vulnerability (pre-auth)
 C) Cross Site Scripting (XSS) Vulnerabilities (pre-auth, reflected)
 D) Cross Site Scripting (XSS) Vulnerabilities (post-auth, reflected)
```

Vtiger CRM 5.2.0 Code Execution / Cross Site Scripting / Local File Inclusion

Related Vulnerabilities: CVE-2010-3909 CVE-2010-3910 CVE-2010-3911
Publish Date: 18 Nov 2010
Author: Alessandro Tanasi, Giovanni Pellerano
Source

```
Vtiger CRM 5.2.0 Multiple Vulnerabilities

 Name              Multiple Vulnerabilities in Vtiger CRM
 Systems Affected  Vtiger CRM 5.2.0 and possibly earlier versions
 Severity          Medium
 Impact (CVSSv2)   Medium 9/10, vector: (AV:N/AC:L/Au:N/C:P/I:P/A:C)
 Vendor            http://www.vtigercrm.com
 Advisory
http://www.ush.it/team/ush/hack-vtigercrm_520/vtigercrm_520.txt
 Authors           Giovanni "evilaliv3" Pellerano (evilaliv3 AT ush DOT it)
                   Alessandro "jekil" Tanasi (alessandro AT tanasi DOT it)
 Date              20101116

I. BACKGROUND

Vtiger CRM is a free, full-featured, 100% Open Source CRM software ideal
for small and medium businesses, with low-cost product support available
to production users that need reliable support.

II. DESCRIPTION

Multiple Vulnerabilities exist in Vtiger CRM software.

III. ANALYSIS

Summary:

 A) Remote Code Execution (RCE) Vulnerability
 B) Local File Inclusion (LFI) Vulnerability (pre-auth)
 C) Cross Site Scripting (XSS) Vulnerabilities (pre-auth, reflected)
 D) Cross Site Scripting (XSS) Vulnerabilities (post-auth, reflected)

A) Remote Code Execution (RCE) Vulnerability

A Remote Code Execution vulnerability exists in Vtiger CRM version 5.2.0.
In order to exploit this vulnerability an account on the CRM system is
required.

The vulnerability resides in the "Compose Mail" section. The software
permits sending email with attachments and offers a draft save feature.
When this feature is used and an attachment is specified, the
"sanitizeUploadFileName($fileName, $badFileExtensions)" validation routine
is called.

This routine involves some security checks to handle uploaded files, it
does blacklist extension checking and if a bad extension is detected the
txt extension is appended to the file-name.

The blacklist array, defined inside config.inc.php, lacks the "phtml"
extension,
well known to be supported by some distributions and packaging, allowing an
attacker to execute the uploaded file and causing the vulnerability.

Below is the blacklist array defined in config.template.php:

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&l

112: $upload_badext = array('php', 'php3', 'php4', 'php5', 'pl', 'cgi',
'py',
     'asp', 'cfm', 'js', 'vbs', 'html', 'htm', 'exe', 'bin', 'bat',
'sh', dll',
     'phps');

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&l
```

```
For the exploitation methodology for this issue we remand to [1], a
previous advisory of ours.

B) Local File Inclusion (LFI) Vulnerability (pre-auth)

A Local File Inclusion vulnerability exists in Vtiger CRM version 5.2.0.
The vulnerability can be exploited by unauthenticated users.

The vulnerability is present due to insecure statements in the script
phprint.php that forward unfiltered user inputs directly to an include()
function call.

Below are the insecure statements in phprint.php:

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

61: $lang_crm = (empty($_GET['lang_crm'])) ? $default_language :
$_GET['lang_crm'];
62: $app_strings = return_application_language($lang_crm);

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

Where the function return_application_language() is defined in
include/utils/utils.php as follows:

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

427: function return_application_language($language)
428: {
  /.../

435:    @include("include/language/$language.lang.php");

       /.../
464: }

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

The same issue is also present in graph.php:

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

47: if(isset($_REQUEST['current_language']))
48: {
49:        $current_language = $_REQUEST['current_language'];
50: }
51:
52: // retrieve the translated strings.
53: $app_strings = return_application_language($current_language);

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

The two vulnerable flaws can be triggered, for example, using:

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

curl -kis "http://127.0.0.1/vtigercrm/phprint.php?lang_crm=/../[..]/../
etc/passwd%00&amp;module=a&amp;action=a&amp;activity_mode=

curl -kis
"http://127.0.0.1/vtigercrm/graph.php?current_language=/../[..]/../
etc/passwd%00&amp;module=Accounts&amp;action=Import&amp;parenttab=Support"

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

C) Cross Site Scripting vulnerabilities (pre-auth, reflected)

A reflected XSS vulnerability exists in Vtiger CRM version 5.2.0.
The vulnerability can be exploited against unauthenticated users only.

The vulnerability is present on the login form, and can be triggered
using these inputs:

    - username:  " onmouseover="javascript:alert('XSS');
    - password:  " onmouseover="javascript:alert('XSS');

PoC URL that exploits this vulnerability:

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&l

http://127.0.0.1/vtigercrm/index.php?module=Users&amp;action=Login&amp;default_user_name
```

```
=%22%20onmouseover=%22javascript:alert('XSS');

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

D) Cross Site Scripting (XSS) Vulnerabilities (post-auth, reflected)

A reflected XSS vulnerability exists in Vtiger CRM version 5.2.0.
The vulnerability can be exploited against authenticated users only.

The vulnerability is present due to insecure statements in the script
modules/Settings/GetFieldInfo.php that reflect unfiltered user inputs
inside the page output.

PoC URL that exploits this vulnerability:

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

http://127.0.0.1/vtigercrm/index.php?module=Settings&amp;action=GetFieldInfo&amp;label
=%3Cscript%3Ealert(123)%3C/scrip%3E

--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--8&lt;--

IV. DETECTION

Vtiger CRM 5.2.0 and possibly earlier versions are vulnerable.

Vtiger CRM can be identified using the following google dork:

    - intitle:"vtiger CRM 5 - Commercial Open Source CRM"

V. WORKAROUND

No fix available.

VI. VENDOR RESPONSE

"We were able to reproduce the issues you reported on 5.2,
and are working on releasing a security update shortly.
We expect to release this update within the next 3 to 4 weeks,
after running some more tests."

VII. CVE INFORMATION

CVE-2010-3909 [A]
CVE-2010-3910 [B]
CVE-2010-3911 [C, D]

VIII. DISCLOSURE TIMELINE

20101009 Bugs discovered
20101012 First vendor contact
20101012 Vendor response (Sreenivas Kanumuru)
20101012 Contacted Steven M. Christey (mitre.org)
20101012 CVEs assigned by Steven M. Christey
20100102 Vtiger CRM team confirms vulnerability (Sreenivas Kanumuru)
20101015 Advisory release scheduled for 20101115
20101116 Advisory released

IX. REFERENCES

[1] Vtiger CRM 5.0.4 Multiple Vulnerabilities
    http://www.ush.it/team/ush/hack-vtigercrm_504/vtigercrm_504.txt

X. CREDIT

Giovanni "evilaliv3" Pellerano, Alessandro "jekil" Tanasi are credited
with the discovery of this vulnerability.

Giovanni "evilaliv3" Pellerano
web site: http://www.ush.it/, http://www.evilaliv3.org/
mail: evilaliv3 AT ush DOT it

Alessandro "jekil" Tanasi
web site: http://www.tanasi.it/
mail: alessandro AT tanasi DOT it

XI. LEGAL NOTICES

Copyright (c) 2010 Francesco "ascii" Ongaro

Permission is granted for the redistribution of this alert
```

```
electronically. It may not be edited in any way without mine express
written consent. If you wish to reprint the whole or any
part of this alert in any other medium other than electronically,
please email me for permission.

Disclaimer: The information in the advisory is believed to be accurate
at the time of publishing based on currently available information. Use
of the information constitutes acceptance for use in an AS IS condition.
There are no warranties with regard to this information. Neither the
author nor the publisher accepts any liability for any direct, indirect,
or consequential loss or damage arising from use of, or reliance on,
this information.

<p>
```

Vulmon Search

Vulmon Search is a vulnerability search engine. It gives comprehensive vulnerability information through a very simple user interface.

About

Home
Recent Vulnerabilities
Product List
Vendor List
Research Posts
Trends
Blog
About
Contact

Products

Vulmon Search
Vulmon Research
Vulmon Alerts
Vulmap

Connect

Twitter
Reddit
Linkedin
Facebook