



Enterprise-ready Open Source

Vtiger CRM 5.0.4 Update-1 Release Notes

Table of Contents

| | |
|--|---|
| 1. About vtiger 5.0.4 - Update 1 | 3 |
| 2. Changes Log | 4 |
| 3. Contact Information | 5 |

1. About vtiger 5.0.4 – Update 1

Vtiger CRM 5.0.4 Update-1 Patch addresses key security and some critical bug fixes.

Special thanks to - **Mark Piper, Fabian Fingerele, and Different Solutions** - for the key contributions

Download link for the patch:

http://prdownloads.sourceforge.net/vtigercrm/VtigerCRM504_Security_Patch.zip?download

How to Apply the Patch:

- 1. Backup the existing Vtiger source directory.**
- 2. Unzip the patch into your existing VtigerCRM source directory.**

2. Changes Log

Following is the link of the security vulnerabilities fixed and provided in the patch:

Security Issues:-

- **Local File Disclosure** - VtigerCRM 5.0.4 is vulnerable to local file contents disclosure. This vulnerability may exist in earlier versions as well. A malicious user may exploit this vulnerability to disclose potentially sensitive information. The flaw is caused due to a lack of input validation of the file URL parameter when evaluated in the CommonAjax.php file. By modifying the file parameter path, and in turn terminating it with a NULL byte, it is possible to trick CommonAjax.php into including files which do not include '.php' in the file name.
- **Cross-Site Scripting** - VtigerCRM 5.0.4 is vulnerable to local file contents disclosure. This vulnerability may exist in earlier versions as well. A malicious user may exploit this vulnerability to disclose potentially sensitive information. The flaw is caused due to a lack of input validation of the file URL parameter when evaluated in the CommonAjax.php file. By modifying the parenttab URL parameter value, it is possible to include malicious JavaScript presented to the user.
- **SQL injection Vulnerability** - VtigerCRM 5.0.4 is vulnerable to authenticated SQL injection. This vulnerability may exist in earlier versions as well. A malicious user may exploit this vulnerability to disclose potentially sensitive information or modify the underlying database.
- **Arbitrary File Upload** - VtigerCRM 5.0.4 allows a malicious user to upload and execute malicious PHP files. While vtigerCRM has functionality to prevent users from uploading files with a ".php" extension, this restriction may be bypassed by uploading a file named in upper case (for example: BAD.PHP). Additionally, the file extension ".phtml" is not restricted. PHTML is often associated (by default) with PHP files in many LAMP configurations.

Critical Trac Tickets:-

- [5235](#) - Patch Apply: Timeout settings need change
- [5255](#) - Cannot import more than 500 records
- [5307](#) - Campaign Related info getting lost
- [5298](#) - File attachment download gets corrupted
- [5294](#) - Organization image upload issue
- [5231](#) - Webmail qualify issue
- [5268](#) - Homepage dashboard link showing incorrect data in list view
- [4847](#) - Problem in selecting users/groups/profiles from the roles and groups edit view
- [5393](#) - Not able to delete default profiles/roles/users

3. Contact Information

Important Emails

- Information: info@vtiger.com
- Sales: sales@vtiger.com
- Services: services@vtiger.com
- Partnership: partnership@vtiger.com
- Webmaster: webmaster@vtiger.com

vtiger Network

- vtiger Corporate Site: www.vtiger.com
- Developer Blogs: <http://blogs.vtiger.com>
- Customer Support: <http://portal.vtiger.com>
- vtiger CRM Demo: <http://en.vtiger.com>
- Community Forums: <http://forums.vtiger.com>
- Wiki Documents: <http://wiki.vtiger.com>
- Issue Tracker: <http://trac.vtiger.com>
- Community Projects: <http://forge.vtiger.com>
- Developer Mailing List: <http://lists.vtiger.com>
- Jobs Board: <http://jobs.vtiger.com>

More details can be found on our [site](#).