

RCE exists in Ionize-V1.0.8.1 'install/class/Installer.php' file #L1035 #403



Overflow opened this issue on Feb 24 · 1 comment

Overflow 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

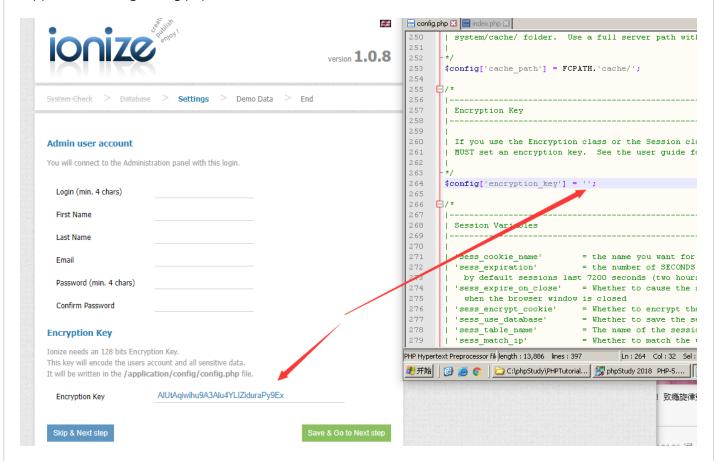
Where the vulnerability occurs:

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

```
@ github.com/ionize/ionize/blob/master/install/class/Installer.php#L1035
        1027
                       */
        1029
                       function _save_user()
                              // Config library
        1031
                              require_once('./class/Config.php');
        1033
                               // 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');
                                       if ($config['encryption_key'] == '')
        1040
        1042
                                               $conf = new ION_Config(APPPATH.'config/', 'config.php');
                                               $conf->set_config('encryption_key', $_POST['encryption_key']);
        1044
                                               if ($conf->save() == FALSE)
        1046
        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"

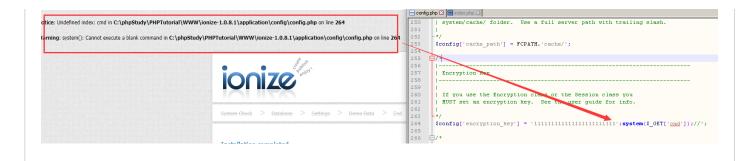


payload:

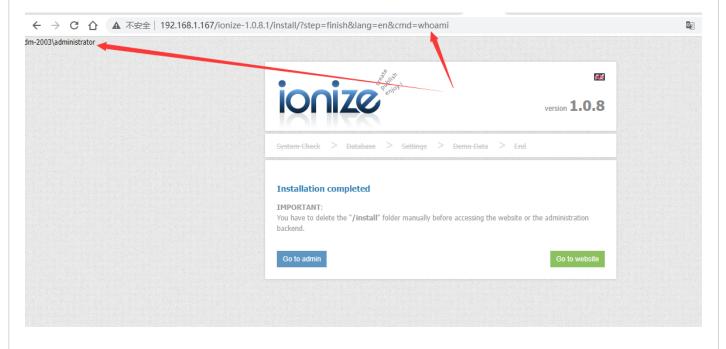
Enter payload to submit

ionize	version 1.0
System Check > Databas	se > Settings > Demo Data > End
Admin user account	
You will connect to the Admini	istration 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 Encry This key will encode the users It will be written in the /appli	account and all sensitive data
	11111111111111111111111111111111111111

Ok, the payload has been successfully written into



try command execution



Bugfix

Only letters and numbers are allowed, no other characters are allowed



Overflow closed this as completed on Mar 31

partikule commented on Mar 31

Member

Thanks.

Ionize is a dead project since around 2017...

٠	٠	٠

ssignees
lo one assigned
abels
lone yet
rojects
lone yet
/lilestone
lo milestone
Development Development
lo branches or pull requests

2 participants



