Abysssec Research

1) Advisory information

Title	**: Cpanel PHP Restriction Bypass Vulnerability**
Version	**: <= 11.25**
Discovery	**: http://www.abysssec.com**
Vendor	**: http://www.cpanel.net**
Impact	**: Ciritical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- Restriction Bypass Vulnerability

Impact

Attackers can use this issue to gain access to restricted files, potentially obtaining sensitive information that may aid in further attacks.It can help attacker to bypass restriction such as mod_security , Safemod and disable functions.

Remotely Exploitable

No

Locally Exploitable

Yes

3) Vulnerability details

1- Restriction Bypass Vulnerabilities:

Load your file with this style:
[Domain | Filename]
Located in :
/home/[user directory name/.fantasticodata/[Script name folder] and include all file.

Example:
/home/yoursite/.fantasticodata/Joomla_1.5/
then include this file :
test.com|file1

After you created your malicious file in that style you can browse this page:

http://test.com:2082/frontend/x3/fantastico/autoinstallhome.php?app=Joomla_1.5

Now your PHP code will execute without /safe_mode/Disable_function/ Mod_security due to cpanel php.ini must be run with execute permission.

Vulnerable code located in in /usr/local/cpanel/3rdparty/fantastico/autoinstallhome.php :

```
Line 529 :
 function Show_Notice ( $Script , $Version_Numbers )
  {
     $Home_Directory = $GLOBALS['enc_cpanel_homedir'] ;
     if ( substr ( $Home_Directory , -1 ) != '/' )
     {
        $Home_Directory = $Home_Directory . '/' ;
     }
     $Files = Array ( ) ;
[This Place]   --->    $Directory = $Home_Directory . '.fantasticodata/' . $Script . '/' ;
     $Files = Get_Files ( $Directory ) ;
     if ( !empty ( $Files ) AND is_array ( $Files ) )
     {
        $Temporary = natcasesort ( $Files ) ;
```

```
    }
    foreach ( $Files As $File )
    {
      $Name    = '' ;
      $Path    = '' ;
      if ( strstr ( $File , "|" ) )
      {
        $Name = explode ( "|" , $File ) ;
        $Name = $Name[1] ;
      }
      else
      {
        $Name = $File ;
      }
      /* Debugging */ // echo $Directory . $File . '<br/>' ;
      if ( is_file ( $Directory . $File ) )
      {
        include $Directory . $File ;
        if ( !empty ( $thisscriptpath ) )
        {
          $Path = $thisscriptpath ;
        }
        else
        {
          $Path = $Home_Directory . 'public_html/' . $Name . '/' ;
        }
        if ( substr ( $Path , -1 ) != '/' )
        {
          $Path = $Path . '/' ;
        }
        /* Debugging */ // echo $Path . 'fantversion.php<br/><br/>' ;
        if ( is_file ( $Path . 'fantversion.php' ) )
        {
          include $Path . 'fantversion.php' ;
          if ( !empty ( $version ) )
          {
            if ( in_array ( $version , $Version_Numbers ) )
            {
              return 'Yes' ;
            }
          }
        }
      }
    }
    return 'No' ;
  }
```