[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

Re: Buffer Overflows in cmd.cc

From: Antonio Ceballos
Subject: Re: Buffer Overflows in cmd.cc
Date: Tue, 6 Apr 2021 08:37:36 +0200

Hi Michael,

Thank you for your bug report. I think you are correctly spotting a problem.
In fact, similar bugs were found in the past. Thank you very much for your
patch too, and for the hint to reproduce the bug. We will review it all in detail
for a future release fixing the problem.

Regards,
Antonio Ceballos

On Mon, Apr 5, 2021 at 5:54 AM Michael Vaughan (RIT Student) <mav8557@rit.edu> wrote:

> Hello,
>
> I wanted to report a potentially exploitable issue within the cmd_pgnload() and cmd_pgnreplay() functions in cmd.cc. In the loop between lines 482-485 in the former function, a specially crafted epdline could overrun the data buffer located here:
>
> ```
> char data[MAXSTR]="";
> char epdline[MAXSTR]="";
>
> /* snip */
>
> int i=0;
> while ( epdline[i] != '\n' ) {
>   data[i+9] = epdline[i];
>   ++i;
> }
> ```
>
> Since this loop only ends when there is a newline within epdline, the end of the data buffer is not checked and the program will continue to copy bytes into and past the buffer, eventually overwriting the return address on the stack. A PGN file that exploits this bug is potentially possible, but it is easier to reproduce this in gdb by setting a breakpoint on the load_pgn_as_epd() function. Then load any compliant file with the pgnload command as follows:
>
> pgnload <*filename*>
>
> If you step after the SaveEPD() call but before the temporary file ".tmp.epd" is opened with fopen(), you can write to (or replace) the temporary file with a buffer overflow payload, like two hundred of "A". Continuing the program will cause it to open and copy this into the 128 byte data buffer, overflowing it and overwriting the return address, as well as any stack cookie or other data in the way. This code is mirrored in the cmd_pgnreplay() function also, and can be mitigated in the same way. It should be reproducible there using the same steps.
>
> I have attached a patch to this email with a potential fix to this issue. I hope this finds you well.
>
> Regards,
>
> Michael Vaughan

reply via email to

Antonio Ceballos

[Prev in Thread] **Current Thread** [Next in Thread]

- **Buffer Overflows in cmd.cc**, *Michael Vaughan (RIT Student)*, 2021/04/04
  - **Re: Buffer Overflows in cmd.cc**, *Antonio Ceballos* **<=**

- Prev by Date: **Buffer Overflows in cmd.cc**
- Previous by thread: **Buffer Overflows in cmd.cc**
- Index(es):
  - **Date**
  - **Thread**