CVE-2016-10128

描述：Buffer overflow in the git\_pkt\_parse\_line function in transports/smart\_pkt.c in the Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to have unspecified impact via a crafted non-flush packet.

软件： libgit2

源码： src/transports/smart\_pkt.c

出现位置：427-432 行

关键源码：

if (bufflen > 0 && bufflen < (size\_t)len)

return GIT\_EBUFS;

+ /\*

+ \* The length has to be exactly 0 in case of a flush

+ \* packet or greater than PKT\_LEN\_SIZE, as the decoded

+ \* length includes its own encoded length of four bytes.

+ \*/

+ if (len != 0 && len < PKT\_LEN\_SIZE)

+ return GIT\_ERROR;

+

line += PKT\_LEN\_SIZE;

/\*

\* TODO: How do we deal with empty lines? Try again? with the next