Security vulnerability reports as a way to establish your 133t kr3|)z

devblogs.microsoft.com/oldnewthing/20121127-00

November 27, 2012



Raymond Chen

There is an entire subculture of l33t l4xors who occasionally pop into our world, and as such have to <u>adapt their communication style to match their audience</u>. Sometimes the adaptation is incomplete.

```
I have appended a file exploit.pl which exploits a vulnerability
in XYZ version N.M. The result is a denial of service.
The perl script generates a file, which if double-clicked,
results in a crash in XYZ.
S00PrA\/\/e$Um#!/usr/bin/perl
system('cls');
system('color c');
system('title XYZ DOS Exploit');
print('
                          $ | |
   $$$
');
sleep 2;
system('cls');
print('
                            $$$
   -- | | | | __ | | / \/ \ $$$ | |
  - - | |
                            $$$
The exploit!
');
sleep 2;
text{the exploit} = "\0";
open(file, ">exploit.xyz");
print(file $theexploit);
system('cls');
print('
                           $ | |
                |__| \ /\ /
                            $$$ | |
   -- | | | |
   |--|r||\/\/e $ - m *
                            $$$
```

You may have trouble finding the exploit buried in that perl script, because the perl script consists almost entirely of graffiti and posturing and chest-thumping. (You may also have noticed a bug.) Here is the script with all the fluff removed:

```
$theexploit = "\0";
open(file, ">exploit.xyz");
print(file $theexploit);
```

This could've been conveyed in a simple sentence: "Create a one-byte file consisting of a single null byte." But if you did that, then you wouldn't get your chance to put your name up in lights on the screen of a Microsoft security researcher!

(For the record, the issue being reported was not only known, a patch for it had already been issued at the time the report came in. The crash is simply a self-inflicted denial of service with no security consequences. There isn't even any data loss because XYZ can open only one file at a time, so by the time it crashes, all your previous work must already have been saved.)

Raymond Chen

Follow

