

[Full-Disclosure] Test your windows OS

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0065.html>

From: Berend-Jan Wever (*skylined_at_edup.tudelft.nl*)

Date: 10/04/04

To: <full-disclosure@lists.netsys.com>

Date: Mon, 4 Oct 2004 17:39:06 +0200

Hi all,

Wanna do a quick test to see if the programmers that wrote your windows operating system have any clue as to what they're doing? Run these commands from cmd.exe in the system32 directory:

```
for %i in (*.exe) do start %i %n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n
for %i in (*.exe) do start %i AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA....
(type as much "A"-s as cmd.exe allows on one line.)
```

Each command will execute every program in your system32 directory, most of them will either ignore the parameter or report an error because the parameter doesn't make sense... But on my win2k system I found 6 programs vulnerable to these very simple formatstring and BoF tests.... grpconv even gives EIP 0x00410041, can it be any easier?

These are not vulnerabilities in itself: you cannot gain access or elevate privileges but I just wanted to let you know that these programmers did a sloppy job.

Cheers,
SkyLined

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>