

## Re: Priviledge escalation attack

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-10/0043.html>

---

**From:** Knud Erik Højgaard ([knud@skodliv.dk](mailto:knud@skodliv.dk))

**Date:** 10/28/02

From: Knud Erik Højgaard <[knud@skodliv.dk](mailto:knud@skodliv.dk)>

To: <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

Date: Mon, 28 Oct 2002 18:37:10 +0100

> *From: "Eric Howard" [dlydl7502@sneakemail.com](mailto:dlydl7502@sneakemail.com)*

[snip]

> *Scenario:*

>

> *I (who am logged in as Administrator) am having a network connectivity*

> *problem. I drop to a command line prompt and type 'nbstat', that*

> *right 'nbstat', which is a typo. A batch file in the WINNT directory*

> *created by user with normal access privileges called 'nbstat.bat'*

> *executes. It dutifully reports "'nbstat' is not recognized as an*

> *operable program or batch file." and executes whatever code it wants with*

> *Administrator privileges. The fake error message pretty much guarantees I*

> *won't notice this.*

>

> *Far fetched? Ask yourself if you have ever made a typo at the Command*

> *line? Microsoft has made a GRAVE ERROR by allowing a system directory to*

> *be world writeable. People need to be aware of this problem and some*

> *action needs to be taken so this can be fixed.*

Naming a file cmd.exe and placing it in the root of %SYSTEMDRIVE% will happily run this instead of the one in %SYSTEMROOT% if 'cmd' is invoked from the start/run box, regardless of my systemdrive (E:) being later in the path than my systemroot. I believe this is old news...

--

Knud Erik Højgaard

---

- **Previous message:** [Eric Howard: "Priviledge escalation attack"](#)
- **In reply to:** [Eric Howard: "Priviledge escalation attack"](#)
- **Next in thread:** [Mike Coppins: "Re: Priviledge escalation attack"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)