

# RE: Another Low Blow From Microsoft: MBSA Failure!

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-02/0317.html>

---

**From:** Frank Knobbe ([frank\\_at\\_knobbe.us](mailto:frank_at_knobbe.us))

**Date:** 02/11/04

To: Joe DeMarco <[demarcoj@comcast.net](mailto:demarcoj@comcast.net)>

Date: Tue, 10 Feb 2004 19:24:32 -0600

On Tue, 2004-02-10 at 13:26, Joe DeMarco wrote:

> *Maybe it's just me but, I wouldn't consider a patch successfully*  
> *applied*  
> *until the machine is rebooted. Registry changes usually require this*  
> *process.*

I would go even further and question the reliability of just checking for the presence of Registry keys that claim a patch has been installed. Anything short of verifying the MD5 hash of a given DLL, driver file or executable just makes assumptions about a patched version being present or not. Those assumptions tend to come back to haunt you, and I believe there are enough people that had exactly that happening. I remember some patch (a year or so ago) that overwrote a previously patched DLL with a vulnerable version. Anything checking Registry keys, like Windows Update I believe, made the assumption that the system was patched when in fact the defective DLL rendered the system vulnerable.

Any tool, Windows Update, MBSA, or 3rd party should check the actual files in question, not just logfiles or Registry keys (or anything that makes historical statements rather than actual statements).

Regards,  
Frank

- 
- application/pgp-signature attachment: [This is a digitally signed message part](#)