

# IIS

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-10/0163.html>

---

**From:** Leandro Malaquias ([wazup@brnet.com.br](mailto:wazup@brnet.com.br))

**Date:** 10/23/01

From: Leandro Malaquias <[wazup@brnet.com.br](mailto:wazup@brnet.com.br)>

To: [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)

Subject: IIS

Date: Tue, 23 Oct 2001 14:42:46 -0200

Message-Id: <01102314424601.01367@223220>

Wazup,

I'm a security analyst for a company here in brazil and I noticed something odd, so I was wondering if anyone else had this problem aswell and how was it solved.

The company I work for were running IIS 5.0 SP1 with all patches applied (all 3 billion of them hahaaha)

And everything was running smoothly untill they decided to install SP2.

At first all I noticed was that some patches were removed, so I told them to re-apply those patches missing.

The wierd thing was that when they tried to apply the missing patches a pop up error message came up saying that they were not allowed to install patches before the SP2.

I've contacted microsoft but the reply was "READ TECHNET" (in other words they didn't have a clue on what to do).

BY D WAY MICROSOFT I DIDN'T FIND A THING ABOUT THIS PROBLEM IN TECHNET.

So people beware...

The main vulnerabilities that I found after they installed SP2 were:

- Shtml.exe Denial of Service
- Internet Printing Buffer Overflow

Peace in the middle east

Leandro Malaquias

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

## SecurityFocus Penetration: IIS

- **Previous message:** [hellNbak: "Re: IIS : access to cmd.exe and multiple commands on one line"](#)
- **Next in thread:** [miguel.dilaj@pharma.novartis.com: "Re: IIS"](#)
- **Reply:** [miguel.dilaj@pharma.novartis.com: "Re: IIS"](#)
- **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)