

# [NT] IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0056.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/14/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Jul 2004 14:08:28 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

---

## SUMMARY

A buffer overrun vulnerability exists in Internet Information Server 4.0 that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

## DETAILS

Vulnerable Systems:

\* Microsoft Windows NT Workstation 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3A2B38C5-FA73-49EC-9EEF-06FE8D6495C0&dis>

Download the update

\* Microsoft Windows NT Server 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3A2B38C5-FA73-49EC-9EEF-06FE8D6495C0&dis>

Download the update

Immune Systems:

\* Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4

## Securiteam: [NT] IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

- \* Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- \* Microsoft Windows XP 64-Bit Edition Service Pack 1
- \* Microsoft Windows XP 64-Bit Edition Version 2003
- \* Microsoft Windows Server 2003
- \* Microsoft Windows Server 2003 64-Bit Edition
- \* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0205>>  
CAN-2004-0205

The vulnerability exists due to an unchecked buffer in the IIS redirection function. The redirection function can be used by an administrator to redirect an incoming request to a different directory or to another host. Successful explo