

# New attack vectors and a vulnerability dissection of MS03-007

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-03/0053.html>

---

**From:** David Litchfield ([david@NGSSOFTWARE.COM](mailto:david@NGSSOFTWARE.COM))  
**Date:** 03/21/03

Date: Fri, 21 Mar 2003 16:16:16 -0000  
From: David Litchfield <[david@NGSSOFTWARE.COM](mailto:david@NGSSOFTWARE.COM)>  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

The patch announced by Microsoft on the 17th March 2003 fixed a security vulnerability in the core of the Windows 2000 operating system. This flaw was actively being exploited through WebDAV requests to Microsoft's Internet Information Server 5. It must be stressed that IIS was simply the attack vector; the method or route used to actually exploit the flaw. The problem, however, is much wider in scope than just simply machines running IIS. Researchers at NGSSoftware have isolated many more attack vectors including java based web servers and other non-WebDAV related issues in IIS. Due to this, NGSSoftware urge Windows 2000 users to apply the patch.

For a paper that examines the vulnerability in detail, please read <http://www.ngssoftware.com/papers/ms03-007-ntdll.pdf> .

Cheers,  
David Litchfield  
NGSSoftware Ltd  
+44(0)208 401 0070  
<http://www.ngssoftware.com/>

oo  
Delivery co-sponsored by TruSecure Corporation  
oo  
TICSA - Anniversary Special - Limited Time

Become TICSA certified for just \$221.25 US when you register before 3/31/03 with PROMO "TS0103" at [www.2test.com](http://www.2test.com). NO membership fees, certification good for 2 years. Price for international delivery just \$296.25 US, with this offer. Offer cannot be combined with any other special and expires 3/31/03. Visit [www.trusecure.com/ticsa](http://www.trusecure.com/ticsa) for full details.

oo