

Windows kernel overflow fixed

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-04/0044.html>

From: NGSSoftware Insight Security Research (*nistr_at_NEXTGENSS.COM*)

Date: 04/13/05

Date: Wed, 13 Apr 2005 16:50:05 +0100

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

John Heasman of NGSSoftware has discovered a high risk vulnerability in the Microsoft Windows kernel. The vulnerability (CAN-2005-0060) permits a logged-on user to escalate privileges to take full control of the system when Windows processes certain types of font.

Microsoft has developed a patch to fix the problem. More information can be found here:

<http://www.microsoft.com/technet/security/bulletin/MS05-018.msp>

NGSSoftware are going to withhold details about this flaw for three months. Full details will be published on the Tuesday, 12th of July 2005. This three month window will allow Microsoft customers the time needed to test and apply the patch before the details are released to the general public. This reflects NGSSoftware's new approach to responsible disclosure.

Typhon III, NGSSoftware's advanced vulnerability assessment scanner, has been updated to check for and positively identify this flaw. More information about Typhon can be found here:

<http://www.ngssoftware.com/typhon.htm>

NGSSoftware Insight Security Research

<http://www.nextgenss.com/>

+44(0)208 401 0070

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--