

MajorRev: v2.0 Microsoft Security Bulletin MS05-019 – Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service (893066)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-06/0002.html>

From: Cooper, Russ (*russ.cooper_at_CYBERTRUST.COM*)

Date: 06/14/05

Date: Tue, 14 Jun 2005 13:39:22 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS05-019:
Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial
of Service (893066)

Bulletin URL:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-019.msp>>

Reason for Revision: Microsoft updated this bulletin today to advise customers that a revised version of the security update is available. We recommend installing this revised security update even if you have installed the previous version. The revised security update will be available through Windows Update, Software Update Services (SUS), and will be recommended by the Microsoft Baseline Security Analyzer (MBSA).

Version Number: 2.0

Issued Date: Tuesday, April 12, 2005

Revision Date: Tuesday, June 14, 2005

Impact of Vulnerability: Remote Code Execution Maximum Severity Rating:
Critical

Patch(es) Replaced: None.

Caveats: Microsoft Knowledge Base Article 893066 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 893066.

Tested Software:

Affected Software:

* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4 <<http://tinyurl.com/6whdr>>

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 <<http://tinyurl.com/3k9eh>>

* Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)

<<http://tinyurl.com/4gfaz>>

* Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)

<<http://tinyurl.com/4ysty>>

* Microsoft Windows Server 2003

<<http://tinyurl.com/5r7l3>>

* Microsoft Windows Server 2003 for Itanium-based Systems, Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) – Review the FAQ section of this bulletin for details about these operating systems. Windows Server 2003 (all versions) <<http://tinyurl.com/4ysty>>

Technical Description:

* IP Validation Vulnerability – CAN-2005-0048: A remote code execution vulnerability exists that could allow an attacker to send a specially crafted IP message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to remotely execute code. However, attempts to exploit this vulnerability would most likely result in a denial of service.

* ICMP Connection Reset Vulnerability – CAN-2004-0790: A denial of service vulnerability exists that could allow an attacker to send a specially crafted Internet Control Message Protocol (ICMP) message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to reset existing TCP connections.

* ICMP Path MTU Vulnerability – CAN-2004-1060: A denial of service vulnerability exists that could allow an attacker to send a specially crafted Internet Control Message Protocol (ICMP) message to an affected system that could cause network performance to degrade and potentially stop the affected system from responding to requests.

* TCP Connection Reset Vulnerability – CAN-2004-0230: A denial of service vulnerability exists that could allow an attacker to send a specially crafted TCP message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to reset existing TCP connections.

* Spoofed Connection Request Vulnerability – CAN-2005-0688: A denial of service vulnerability exists that could allow an attacker to send a specially crafted TCP/IP message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

Revision History:

* v1.0 – 4/12/2005: Bulletin published

* v1.1 – 5/11/2005: Microsoft updated this bulletin today to advise customers that we plan to re-release the MS05-019 security update in

June, 2005. Until the re-release of this security update is available, customers experiencing the symptoms described in Microsoft Knowledge Base Article 898060 should follow the documented instructions to address this issue. If you are not experiencing this network connectivity issue we recommend that you install the currently available security update to help protect against the vulnerabilities described in this security bulletin.

* v2.0 – 6/14/2005: Microsoft updated this bulletin today to advise customers that a revised version of the security update is available. We recommend installing this revised security update even if you have installed the previous version. The revised security update will be available through Windows Update, Software Update Services (SUS), and will be recommended by the Microsoft Baseline Security Analyzer (MBSA).

This email is sent to NTBugtraq automatically as a service to my subscribers. (v4.01.1975.38886)

Cheers,
Russ Cooper – Senior Scientist – Cybertrust/NTBugtraq Editor

--

NTBugtraq Editor's Note:

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

--