

IBM Internet Security Systems protects against newly discovered Microsoft TCP/IP driver vulnerabilities which could allow denial of service or remote execution.



IBM Internet Security Systems Vulnerability Protection Overview

Vulnerability Overview

In early January 2008, Microsoft announced two serious vulnerabilities in the Microsoft Windows® TCP/IP driver. Both of the vulnerabilities could allow remote code execution and one could allow a remote denial of service (DoS) attack. Two of the driver components affected by these vulnerabilities are enabled by default on Microsoft XP and Vista. Patches are available from Microsoft.

Prior to vulnerability disclosure, IBM Internet Security Systems (ISS) offered protection for all of these vulnerabilities via its Proventia® Intrusion Prevention System (IPS) technologies.

Avenues of Attack

Using the vulnerabilities, an anonymous remote attacker, a bot or remotely controlled host could cause a Denial of Service (DoS) or execute arbitrary code in the TCP/IP driver by sending a specially-crafted sequence of source-specific multicasting (SSM) packets or Internet Control Message Protocol (ICMP) packets.

Since multicast traffic is usually received by multiple destinations, a single attack could target an entire subnet. Even more troubling, attacks targeting these vulnerabilities do not require user interaction to be successful.

Business Impact

Microsoft Windows TCP/IP is the network communication protocol used by all Microsoft operating systems. The widespread use of the Microsoft Windows TCP/IP driver and the lack of user interaction required to complete an attack make these vulnerabilities critical. In addition, the results of a successful attack could be particularly harmful – compromised machines could be ensnared in a botnet and system availability and user productivity could be adversely affected.



Preemptive, Multilayered Protection from IBM ISS

The IBM ISS X-Force® research and development team first discovered the Microsoft vulnerabilities and therefore, IBM ISS clients using Proventia Network IPS were protected ahead of public vulnerability disclosure. By conducting primary research on vulnerabilities, IBM ISS can infuse its products with ahead-of-the-threat protection. IBM Virtual Patch™ technology available in Proventia solutions automatically shields vulnerabilities from attack even before vendor-supplied patches are available. This helps clients avoid emergency patching drills.

IBM ISS also advocates a multilayered protection strategy that provides security from the network core to the perimeter. Applying protection behind firewalls and in between network segments can help prevent sophisticated attacks designed to penetrate a security weakness. Similarly, organizations should apply protection to network elements, servers and desktops for a complete defense-in-depth approach.

Learn More

Additional details about the vulnerabilities can be found in an X-Force Advisory posted here: <http://www.iss.net/threats/282.html>.

To learn more about preemptive, multilayered protection from IBM ISS, call 1 800 776-2362, e-mail sales@iss.net, or visit ibm.com/services/us/iss.

© Copyright IBM Corporation 2008

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.
03-08
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia is a registered trademark of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.