ICMP ping of death (before 1997)

availability

Any host receiving a 64K ICMP payload would crash or reboot

- 64K bytes payload were assumed to be invalid by programmers
- An attacker could split a 64K payload, transmit it and would be reassembled by the receiver overflowing a buffer

Security Bulletin

Microsoft Security Bulletin MS10-009 - Critical

Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)

Published: February 09, 2010 | Updated: February 10, 2010

Version: 1.1

General Information

Executive Summary

This security update resolves four privately reported vulnerabilities in Microsoft Windows. The most severe of these vulnerabilities could allow remote code execution if specially crafted packets are sent to a computer with IPv6 enabled. An attacker could try to exploit the vulnerability by creating specially crafted ICMPv6 packets and sending the packets to a system with IPv6 enabled. This vulnerability may only be exploited if the attacker is on-link.