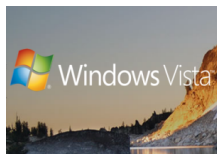


4 June 2008

By: Marius Oiaga, Technology News Editor

Windows Vista
Microsoft

[Linux Cannot Connect to Vista SP1 over Cryptographic Security Services](#)

The IPsec negotiation is at fault

Computers running open source Linux operating systems have problems connecting to Windows Vista Service Pack 1 machines when cryptographic security services are involved. Essentially, the problem affects all distributions of Linux and both Vista RTM and SP1 and is related to failures to establish IPsec connections between the platforms, in scenarios where the connection is initiated from the machine powered by the open source operating system. Internet Protocol security (Ipsec) is, of course, related to the cryptographic security services which are used to protect network communications. "Consider the following scenario. You use Windows Vista Local Security Policy on a Windows Vista-based computer. Or, you use the new Windows Firewall with Advanced Security on a Windows Vista-based computer. You try to initiate an Internet Protocol Security (IPsec) connection from a Linux-based computer to the Windows Vista-based computer. In this scenario, you cannot establish the connection," Microsoft revealed. Previous versions of the Windows operating systems, including Windows XP and Windows Server 2008 have no issues communicating with Linux. The same is valid for IPsec communications between Vista SP1 and Linux, when the connection is initiated by the Vista computer. This is not an interoperability problem, but rather a glitch in Vista SP1. Microsoft offers a hotfix for the customers impacted by this [specific issue](#). "In IPsec negotiation for transform proposal of the combination where Authentication Header (AH) and Encapsulating Security Payload (ESP) are used for securing the same packet (AH+ESP), Windows Vista switches the order and replaces the packet with ESP+AH. This behavior breaks the negotiation. In this case, when you initiate the IPsec connection from a Linux-based computer, the Linux operating system proposes that the IPsec security format is AH+ESP. Therefore, the connection cannot be established," Microsoft explained.