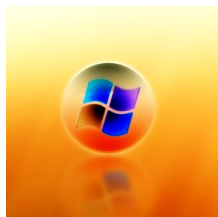


30 November 2006

By: Marius Oiaga, Technology News Editor



Windows Vista Teredo Protocol Vulnerability on Launching Day

The Teredo Protocol: Tunneling Past Network Security and Other Security Implications

You have to agree that timing is everything. And exposing a Windows Vista vulnerability concomitantly with the product's availability via volume licensing to Microsoft's Software Assurance customers gives a new definition to timing. Even more so, since the Redmond Company has applauded over and over again the high level of security introduced by Vista. This is more than the proverbial starting off with the wrong foot; this is a Windows Vista vulnerable to attacks since day one. If you were wondering how much you would have to wait until the first security patch for Windows Vista, the answer may come sooner than you expected. And who do we have to thank for exposing a vulnerability in Windows Vista? Why Symantec of course. In this context, I can't really shake the feeling that Symantec's research paper: *The Teredo Protocol: Tunneling Past Network Security and Other Security Implications* is not only a premeditated action, but one carefully planned and timed. But I don't want to point fingers; It's just a feeling, nothing more. "Teredo is an IPv4 to IPv6 transition mechanism for dual stack hosts that wish to use IPv6 to connect to the Internet, but which are "stuck" behind an IPv4 NAT that doesn't support native IPv6 traffic or 6to4/ISATAP (a fairly common situation). It does this by tunneling the IPv6 traffic through the NAT on top of IPv4 UDP connections and does not require any support at all from the local network," revealed James Hoagland, Principal Security Researcher, Symantec Advanced Threat Research. Teredo is also an open standard developed by Christian Huitema of Microsoft and is integrated and enabled by default in Windows Vista. Symantec is concerned with the security implications of the Teredo protocol. "Even if on the host-side the same security is being applied to Teredo as native IPv6 (as seems to be the case with Vista), security is lowered because: (1) not all network controls may be available or active on the host as well and (2) defense in-depth has been reduced. After all, the network security controls were there for a reason," added Hoagland. Attacks via the Teredo protocol will successfully bypass the network security devices. Firewalls and IDS/IPS will identify IPv6 traffic as UDP traffic on unknown ports. The immediate consequence of this is that security controls will be applied to IPv6 traffic detected as UDP traffic on unknown ports. Symantec concludes that enabled Teredo in Vista will introduce a vector for attacks and a security risk on the network. "Teredo provides a host with a global-scope address and anyone on the Internet can send traffic to the host. Additional security concerns associated with the use of Teredo include the capability of remote nodes to open the NAT for themselves, benefits to worms, ways to deny Teredo service, and the difficulty in finding all Teredo traffic to inspect. Teredo does provide some anti-spoofing mechanisms and is compatible with IPsec, though," concluded Hoagland.