Symantec Voices Security Concerns over Vista's Use of Tunneling Protocol

March 17 2007

Security company Symantec says new research supports fears that Windows Vista's use of the IP tunneling protocol Teredo is potentially insecure.

Microsoft is using Teredo to enable a transition from IPv4, which is the traditional version of the network layer protocol for packet-switched networks now used as the Internet's background, to IPv6, an updated protocol whose biggest benefit is the exponential increase it will bring in the number of IP addresses available for networked devices.

Symantec, based in Cupertino, Calif., first brought up concerns about Teredo in November 2006. As the company points out in its latest report, "Windows Vista Network Attack Surface Analysis" (PDF), Microsoft rewrote the network stack from the ground up in Vista. By doing so, Symantec said, Microsoft has "removed a large body of tested code and replaced it with newly written code, possibly introducing new corner cases and defects."

Oliver Friedrichs, a director at Symantec Security Response, said the introduction of Teredo - one of those newly written, potentially buggy pieces of code - has "a number of security implications."

"Many firewalls and intrusion detection systems are not Teredo-aware," Friedrichs said in an interview with eWEEK. "They're not familiar with the protocol or how to decapsulate the protocol. That means, for one, when we're talking about a firewall, Teredo may allow attacks to

circumvent or bypass the firewall."

Friedrichs said Teredo also presents a problem in that IDSes (intrusion detection systems) are "generally good" at looking at TCP and UDP (User Datagram Protocol) traffic, which are the traditional protocols that transport Web and e-mail requests. If attacks on a system are tunneled, however, they'll be invisible to IDSes, he said.

"Any security device needs to be aware of Teredo in order to look into it and analyze traffic traveling over it," Friedrichs said. "For enterprises, this presents, obviously, a serious concern. Attackers can, for one, tunnel through perimeter devices without being seen and tunnel attacks over - Teredo - without being seen by perimeter devices."

Such perimeter devices include firewalls and routers, such as those from Linksys, he said. "The firewall is traditionally there to filter traffic, but with Teredo it's rendered in many cases ineffective," he said.

Friedrichs said Symantec expects most enterprises to disable Teredo. "That said, we expect it to be enabled on consumer desktops," he said. "It's dormant by default but can be turned on easily."As a matter of fact, Friedrichs said, Symantec found in testing that Teredo is easily activated when a Windows Vista application attempts to use IPv6. "Our findings have shown that Vista in some cases enables Teredo on its own, with no intervention, soon after Vista has been installed," he said.

Friedrichs said Symantec expects attackers to concentrate on hacking Vista with third-party applications as well as directly.

"Microsoft has done some good things in that they've made the core operating system far more secure, so that will have the benefit of eliminating some widespread attacks against Windows like we've seen in the past," he said. "That causes attackers to move from the operating

system to third-party applications, such as drivers. Attackers will focus on those to find vulnerabilities."

Others in the security field, including Coseinc Security Researcher Joanna Rutkowska and BreakingPoint Systems Security Researcher HD Moore, say they agree that drivers are a weakness. "It can be a graphics card with a stupid bug" that opens Vista to attack, Rutkowska said during a panel at Ziff Davis Enterprise's Security Summit 2007. "You can't do anything about it. You can't sue the vendor for introducing a bug. You can't prove it was done intentionally."

"It's certainly a much larger problem than protecting - even - a large operating system," Friedrichs said. "We're looking to every third-party software vendor to secure their products. Attackers are just going to move on" if Vista proves too hard to hack, he said.

One example of a third-party service that has been compromised running on Vista is CA's BrightStor backup. Vulnerability researchers at penetration-testing software maker Core Security demonstrated the exploit at the RSA conference in February.

Jim Hahn, a product manager for Microsoft's Windows Client Team, said in a statement that Microsoft, based in Redmond, Wash., "is aware of a report issued several weeks ago by Symantec that provides another analysis of both Beta and RTM versions of networking technologies in Windows Vista. We believe many of the most recent third-party - analyses - of Windows Vista, including this paper, - validate - many of the key design decisions made in the product. We look forward to further discussing the areas where Symantec has noted improvements could be made to benefit customers."