

By: ~~October 2006~~, Technology News Editor

Microsoft Opens Vista's Core

The Redmond Company compromises over the Windows Vista kernel

Symantec and McAfee have been crying monopoly over Microsoft's policies with the Vista Kernel and it paid off. They've got their way. The Redmond Company will open Windows Vista core to third party security developers. "I think these are acceptable compromises," said John Pescatore, analyst for Gartner. "Being a security vendor is new to Microsoft. It's only very recently started to sell security products, and I think they just underestimated this issue. But it took the EU to sort of say something before Microsoft did anything, so I think that shows Microsoft still has a long way to go before it really understands how it has to operate. The clock is already ticking on 64-bit uptake. Users will migrate to 64-bit sooner than most people expect, so if Microsoft slips past the 12-18 month range for SP1, that could be a problem." "Microsoft is still saying the kernel remains unmodifiable," said Joe Wilcox, an analyst with JupiterResearch. "But the APIs will allow access to information going to the kernel. Microsoft's saying 'don't mess with the kernel, no one should have access. Microsoft was, and is, in a difficult situation. I'm sympathetic with the vendors' position. On the other hand, Microsoft has to protect the core of the operating system. But even this API thing makes me nervous. What happens if the bad guys start using it? Who is going to get access to this [kernel] information? Will it be to all or just some vendors? If it's just some, someone will cry holy hell over it." And yet again, the European Antitrust Commission is the root of another anti-monopoly decision that follows what Microsoft called "constructive dialog." Consequently, the Redmond Company agreed to compromise. It will deliver an array of APIs to permit third-party security solutions developers access to Vista's kernel. And it will also tweak Vista's security status dashboard -- Windows Security Center via additional APIs in order to offer support for outside dashboards. "While we're encouraged by the announcement," said Chris Paden, a Symantec spokesman, "we have not seen the technical information we need to address our concerns about PatchGuard and the Windows Security Center. Vista is supposed to ship to manufacturing within weeks, so we need that information yesterday. If they're willing to commit to a deadline, that would alleviate some of our concerns. These are technical issues. Until we actually see the APIs, all we know is what they have said in the media. So far they have not done anything yet." "We do not want vendors... accessing the kernel through unmodified approaches or modifying the kernel. We will not allow them to go on the fly and modify the kernel, basically circumventing PatchGuard. We need to work with them on the right approaches to work with PatchGuard", said Adrien Robinson, a director in Microsoft's Security Technology Unit.