

Feeling insecure about Vista

Vendors want firm timeline for core workaround code

By: Mari-Len De Guzman

ComputerWorld Canada (10 Nov 2006)

Despite assurances from Microsoft Corp., security vendors are still wary that the software giant has not given a definite timeline for releasing API code to allow third-party security software to work around the Windows Vista OS kernel protection for 64-bit systems.

It is apparent that the API (application programming interface) won't ship with Vista when it launches before the end of the year and will most likely be released with Vista Service Pack 1, said Ari Hypponen, CTO for Helsinki-based F-Secure Corp.

The problem is timing, said Hypponen, adding that despite press announcements, Microsoft has yet to give any specifics as to when such APIs will be available for security vendors.

"The API does not even exist (yet). Nobody knows what the API looks like, whether it will contain all the things that the vendors expect. Microsoft is obviously in control of all that," he said.

Antivirus vendors have aired concerns about certain Vista security features they say compromise the performance of their own products on Vista machines. One is a security management element called Windows Security Center (WSC), which they said can result in customers getting confusing security messages.

Microsoft had refused to allow this feature to be disabled by third-party software until last month, when the Vista creator finally budged and announced it will release API code for WSC.

The second concern is around the PatchGuard, or Kernel Patch Protection, feature for the 64-bit version of Vista and Windows XP. PatchGuard prevents any form of third-party access to the 64-bit kernel. Despite pleas from security vendors, Microsoft has remained firm on that policy.

"[Microsoft has] no intention to allow any third party to modify the kernel, (but) so far, modifying the kernel has been the only way to implement some features of the security suite that all the major vendors are shipping," explained Hypponen.

Microsoft has proposed to create a number of APIs for security vendors to get the kernel functionality they need. While they welcomed this, security vendors now press the software giant to commit to specific timeline for the APIs.

According to Hypponen, industry analysts believe that if the APIs do come as part of the first Vista Service Pack, it could take as long as two years for the security vendors to get their hands on the PatchGuard workaround.

"That's a pretty long window of vulnerability," he said.

Symantec said its discussions with Microsoft are continuing.

"The establishment of a schedule by Microsoft for disclosing in a timely manner the detailed technical information that security providers need to resolve the PatchGuard issue is the specific goal of Symantec," the company said in a statement.

The antivirus vendor, however, declined to comment further beyond the prepared statement.

McAfee, on the other hand, had stronger words for Microsoft. "We have been greatly disappointed by the lack of action by the company so far and Microsoft has not lived up, either in detail or in spirit, to the hollow assurances offered by their top management [earlier]," said Christopher Thomas, a partner at Lovells, McAfee's litigation counsel in Brussels.

Despite security vendors' assertions that the Kernel Patch Protection feature may affect their products' performance and pose security risks to their customers running 64-bit Vista and Windows XP, some Canadian IT professionals are not as concerned.

"[The PatchGuard] is a good measure to prevent things like rootkits and malware getting into the kernel. Those are positive elements from a user perspective," said Stephen Ibaraki, vice-president of the Canadian Information Processing Society, an association of IT professionals.

Microsoft's policy of limiting access to the OS core for stability and security is a "good thing from a user's standpoint," Ibaraki said. "Anything that enhances security within the organization needs to be encouraged."

He expressed confidence the ongoing dispute will "eventually quiet down," citing Microsoft's long history of being able to work with third-party vendors. Microsoft did not respond to interview requests for this article.

QuickLink 060971

