EldoS Provides Raw Disk Access for Vista and XP

By ITPro Today

Published: 2007-03-14 · Archived: 2026-04-05 18:36:35 UTC

Security component maker EldoS announced the availability of RawDisk, a raw disk access driver for Windows Vista and Windows XP systems. Fortunately, the company won't make the product publicly available.

With the advent of XP, Microsoft introduced restrictions that prevent raw disk access for applications that aren't run with administrator-level authority. The company went a step further with Vista by preventing raw disk access for all user-mode processes. The change effectively prohibits people from editing disk sectors to change content.

That sort of protection is useful in some cases. For example, in 2006, security researcher Joanna Rutkowska figured out a way to inject a rootkit into Vista. Rutkowska's technique, called Blue Pill, basically forces Windows to page memory to disk where that memory can then be manipulated by editing raw disk sectors. After changes are made to the paged memory, Windows could be coaxed into calling instructions in that memory space, thereby allowing the changed code to begin executing--and Vista would be none the wiser that the exploit had occurred.

Legitimate tools such as some disk defragmentation programs do need to have raw disk access. The developers of such tools for Vista need to provide their own methodology because the native ability for raw disk access is no longer present as it was in Windows versions prior to Vista.

EldoS said its new raw disk access driver allows raw disk access for both administrative-level and limited-access user accounts.

"We have developed kernel-mode drivers for both 32-bit and 64-bit versions of Windows. Demand for such a solution is high, because preparing the applications for Windows Vista appeared to be a daunting task for many developers," said Eugene Mayevski, EldoS CTO. "Many system utilities stopped working under the new operating system. No solution for the problem was yet offered by Microsoft. For the majority of developers of various utility applications, creation of their own kernel-mode driver is not possible, as it requires the presence of special qualifications and investment of time."

Entities that want to obtain a copy of the EldoS RawDisk driver must contact EldoS directly. The requesting company must have an established business with software already on the market and must explain to EldoS how it intends to use the driver with the product.

EldoS provides a downloadable demo program that allows a person to verify that the driver does work as advertised. However, the company said that the driver in the demo can't be used with any other application.
