

Microsoft's Windows Vista PatchGuard Changes Will Take Years

Neil MacDonald

Microsoft's plan to change aspects of Windows Vista security to address antitrust concerns is a positive move. But the time frame for PatchGuard changes will span years and cause incompatibility problems in the interim.

Event

On 13 October 2006, Microsoft announced that it will change its upcoming Windows Vista operating system following what it called "constructive dialogue" about antitrust concerns with the European Commission and the Korea Fair Trade Commission. Microsoft confirmed that it is on track to release Windows Vista to volume license customers in November 2006 and to the general market worldwide — including the European Union and Korea — in January 2007.

Analysis

The two changes with specific security implications will affect the following areas of Windows technology:

- **PatchGuard:** PatchGuard, the protection mechanism for the kernel in the 64-bit version of Windows, has been highly problematic for some types of independent software vendors (ISVs) and their customers. Contrary to some press reports, Microsoft will not offer a mechanism for deactivating PatchGuard or a trusted mechanism for "kernel hooking" (Windows system-call interception and kernel dispatch table modification). Microsoft has committed to work with ISVs to develop mutually acceptable mechanisms that will enable legitimate, trusted security software to interact with and control aspects of kernel operation — for example, process creation and termination, memory, anti-tampering and code-loading operations — via documented and supported application programming interfaces (APIs), implemented in much the same way as the Windows Filtering Platform framework. However, these APIs do not yet exist, and the changes will require changes to the 64-bit Windows kernel that will not be complete in time for the initial release of Vista. Moreover, any kernel changes may have a "ripple effect" up the software stack and will require retesting of all of Windows Vista applications. To avoid delaying Vista's release or removing the 64-bit version, Microsoft will work with ISVs to deliver initial capabilities and APIs in this area, which we expect in early 2008, when the first service pack for Vista (SP1) will likely be released, with more complex work and more APIs delivered with SP2 or later. The initial 64-bit version of Vista will be PatchGuard-protected, with no deactivation mechanism or other alternative. Slow desktop migration to 64-bit Windows and problematic driver availability mean that this limitation will affect very few enterprises before it is initially addressed in SP1 — but, if Microsoft is slow to deliver these capabilities or fails to meaningfully collaborate, it risks further antitrust concerns.
- **Windows Security Center:** Microsoft has agreed to change the Windows Security Center — a clearinghouse for security-related status information that does not itself deliver any security functionality — so that ISVs can programmatically disable all Windows Security Center alerting for end users without the requirement for end-user intervention. The process itself cannot be deactivated, and Windows Security Center remains a single location where Microsoft and third-party security applications can query Vista's security status. The mechanism to disable Windows Security Center alerts must be architected — likely using signature-based technology — so that malicious software cannot deactivate it. Microsoft needs to work out an agreement with ISVs so that, when their software is uninstalled or switched off, Windows Security Center alerting is returned to its original state. These changes, which should be relatively straightforward, are expected to be included in the final version of Windows Vista released to manufacturing.

RECOMMENDATIONS

- Enterprises using or considering host-based intrusion prevention system (HIPS) or host-based content monitoring and filtering products: Recognize that many of these products will not deliver full functionality using 64-bit Vista — and that only partial functionality may be available even after SP1's release — and demand detailed information from product vendors about which functions are not supported and which specific threats are not addressed by the missing functionality. Do not plan for initial use of 64-bit Vista if you are using incompatible products for which no suitable alternative exists.
- Enterprises not currently considering HIPS point solutions: Recognize that most converged desktop security software products will include behavioral HIPS capabilities, so migration to 64-bit Windows may be delayed. Ask your incumbent security vendors which, if any, converged security functionality is impacted by PatchGuard.
- Impacted enterprises that have not committed to Vista: Inform Microsoft that you will not make this commitment until a firm release date is set for the first set of kernel-control APIs. If the date and the scope of the initial APIs have not been established within nine months of the initial shipment of Vista, the capability will likely not be ready for SP1.
- ISVs and Microsoft: Accept that stronger protection of the kernel is a good thing. It is time to collaborate meaningfully on mutually agreeable mechanisms for extending kernel functionality in a controlled way and in a specific time frame that helps customers.
- All enterprises: Keep up the pressure. With antitrust concerns temporarily satisfied, Microsoft may feel less pressure to make kernel modifications quickly. Pressure ISVs and Microsoft to work together to achieve rapid development of a mutually acceptable, trusted methods of interacting with the Windows kernel, starting with SP1 and evolving over the next several years.
- All enterprises: When evaluating ISVs' security products, demand answers to specific compatibility and interoperability questions, including: Is the product supported on 64-bit Windows? If not, Is the issue PatchGuard-related? Is the vendor actively working with Microsoft on a mutually agreeable set of APIs for kernel control? Is the Windows Security Center alerting and console functionality used, and if not, is the process for other third-party applications that may check Windows Security Center for status information enabled? If Windows Security Center alerting is programmatically disabled, is it restored when the product is uninstalled?

RECOMMENDED READING

- "McAfee Ad Highlights Ongoing Microsoft Security Skirmish" — Microsoft should work with vendors of security products to develop a method of extending kernel functionality. **By Neil MacDonald and John Pescatore**
- "Events Aligning to Make Vista Delay More Likely" — Original equipment manufacturers' demands and the problem of multiple code bases could delay worldwide Vista availability. **By Michael Silver, Stephen Kleynhans and David Mitchell Smith**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509