Firmware Corruption of Memory During Sleep Transitions

June 12, 2009

Abstract

This paper provides information for system manufacturers and firmware developers about firmware corruption of memory during sleep transitions. During Windows® 7 development, multiple Windows-based platforms have encountered memory corruption in the lowest 1 MB of physical memory after resuming from sleep. This document describes the potential root causes of the memory corruption, diagnostic events in Windows 7 that can identify the corruption, and steps to resolve the problem on affected platforms.

This information applies to the following operating systems:
 Windows Server® 2008 R2
 Windows 7

The current version of this paper is maintained on the Web at:
 <http://www.microsoft.com/whdc/system/platform/firmware/mem-corrupt.mspx>

Disclaimer: This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Change |  |  |  |
| June 15, 2009 | First publication |

Contents

[Overview 3](#_Toc232823419)

[Firmware Memory Corruption in Previous Versions of Windows 3](#_Toc232823420)

[Diagnostic Events in Windows 7 and Windows Server 2008 R2 3](#_Toc232823421)

[Resolution Steps 5](#_Toc232823422)

[Call to Action 5](#_Toc232823423)

# Overview

Sleep transitions are critical for extending mobile PC battery life and enabling efficient idle operation for desktop PCs. Platform firmware, attached devices, drivers, and installed software can all affect the reliability and performance of sleep transitions.

During Windows development, we observed some systems that corrupt the lowest 1 MB of physical memory during a sleep transition. We traced the memory corruption to code defects in platform firmware. Because of the pervasiveness of the problem in the industry and the desire for reliable sleep transitions, Windows no longer stores operating system code and data in the lowest 1 MB of physical memory.

To help detect and prevent this firmware code defect, Windows 7 and Windows Server 2008 R2 automatically checksum the contents of the lowest 1 MB of physical memory and log an error event to the system event channel if the memory is corrupted. The event enables system manufacturers and firmware developers to identify the code defect and develop updated firmware. This helps to ensure that future versions of Windows can use all available physical memory for user applications and experiences.

This paper describes the diagnostic event for detecting firmware corruption of memory across sleep transitions. System manufacturers who find this event on their systems must partner with the platform firmware developer to develop updated firmware that resolves the issue. End users who find this event on their system should check with the system manufacturer for updated firmware.

# Firmware Memory Corruption in Previous Versions of Windows

Firmware memory corruption across sleep transitions affects previous versions of Windows, including Windows Vista and Windows XP.

Similar to Windows 7, Windows Vista–based systems do not store operating system code and data in the lowest 1MB of physical memory. This prevents memory corruption on Windows Vista–based systems from negatively affecting the user experience.

However, Windows XP does use the lowest 1 MB of physical memory. Manufacturers should investigate sleep reliability issues on Windows XP–based systems for firmware memory corruption issues. To find the root cause of the reliability problem, install Windows 7 on the system and look for the firmware memory corruption diagnostic that is described in the next section of this document.

Neither Windows Vista nor Windows 7 stores operating system code and data in the lowest 1 MB of physical memory, regardless of whether Windows is running on real or virtualized hardware.

# Diagnostic Events in Windows 7 and Windows Server 2008 R2

Windows 7 and Windows Server 2008 R2 automatically checksum the contents of the lowest 1 MB of physical memory before and after a sleep transition. This checksum process enables Windows to detect memory corruption and report any corruption as an error in the system event log.

If memory corruption occurs in the lowest 1 MB of physical memory during a sleep transition, the hardware application layer (HAL) logs event ID 12 in the Event Viewer, as follows.

|  |  |
| --- | --- |
| Channel | System |
| Level | Error |
| Event source | HAL |
| Event ID | 12 |
| Event message | The platform firmware has corrupted memory across the previous system power transition. Please check for updated firmware for your system. |
| Event data | **Field name** | **Units** | **Description** |
| Count | Count of pages | Number of memory pages detected with corruption |
| First Page | Page number | First page of memory corruption |
| Last Page | Page number | Last page of memory corruption |

The HAL logs the event after each sleep transition in which it detects memory corruption. The event data includes the number of physical memory pages corrupted, the first physical page of corrupted memory, and the last physical page of corrupted memory. Figure 1 shows the properties for such an event.



Figure 1. Properties of memory corruption event ID 12

# Resolution Steps

System manufacturers or firmware developers must investigate and resolve corruption across a sleep transition. In many cases, the resolution of the issue requires a more recent BIOS update for the platform.

System manufacturers should cycle all new Windows-based platforms through sleep transitions and check for the HAL event. If the HAL detects and logs the event, engage the firmware developer to resolve the issue.

Firmware developers can use the event details, including the number of corrupted pages and the first corrupted page, to determine the exact code defect that caused the memory corruption.

# Call to Action

System manufacturers and firmware developers should use the information in this paper to ensure that new platforms do not have memory corruption in the lowest 1 MB of physical memory during a sleep transition:

* System manufacturers should cycle all platforms through sleep transitions and check for HAL event ID 12. If the event occurs, contact the firmware developer to investigate and resolve the issue with a BIOS update.
* Firmware developers should use the detailed data in HAL event ID 12 to determine the code defect that is responsible for the memory corruption.
* Customers who discover this event on their systems should check for updated firmware or BIOS for their system.