

# What could cause a memory corruption bug to disappear in safe mode?

 devblogs.microsoft.com/oldnewthing/20250320-00

alan robinson

March 20, 2025



## Raymond Chen

A customer had a program that crashed occasionally with a heap corruption bug, but in their efforts to isolate the problem, they found that if they ran the program in Safe Mode, the program never crashed. What is so special about Safe Mode that prevents heap corruption bugs? (Can we build the whole airplane out of Safe Mode?)



One of the things that makes Safe Mode safe is that it loads only very basic video drivers. Some parts of video drivers run inside the user-mode process, which means that their memory allocations will intermingle with the process's memory allocations, and it is the nature of heap corruption bugs that small perturbations in memory allocation patterns can drastically alter the way a heap corruption bug manifests itself, possibly even masking it entirely.

The customer knew that they had a heap corruption bug on their hands (and some time with Application Verifier quickly found the source of the corruption). They were just wondering why Safe Mode seemed to hide it.

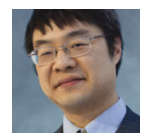
And no, they weren't going to tell their users, "For best results, run this program in Safe Mode."

**Bonus reading:** [Windows Confidential: The Healing Powers of Safe Mode](#), and [The magical healing properties of safe mode – bonus content](#).

## Author

### Raymond Chen

Raymond has been involved in the evolution of Windows for more than 30 years. In 2003, he began a Web site known as The Old New Thing which has grown in popularity far beyond his wildest imagination, a development which still







gives him the heebie-jeebies. The Web site spawned a book, coincidentally also titled The Old New Thing (Addison Wesley 2007). He occasionally appears on the Windows Dev Docs Twitter account to tell stories which convey no useful information.

## 4 comments

---

Discussion is closed. [Login to edit/delete existing comments.](#)

Newest

-  AR  
March 21, 2025  
Sounds a bit like the (possibly apocryphal) story that a version of Word Perfect was shipped to customers in “debug” mode because every attempt to make a release build with optimization and NOPed asserts or whatever was too unstable.  
  
Luckily with modern automated testing techniques that kind of thing would \*never\* happen today.  
  
;-/
-  AD  
Alexander Dyachenko March 21, 2025  
I expect that the video driver must use a completely isolated heap. No?
  -  DK  
Danielix Klimax March 22, 2025  
With GPU drivers things are bit more complex due to performance requirement. Driver is split into two parts. Kernel-mode and user-mode. User-mode gets loaded into (almost) each process and handles graphical calls. They are separate copies, so they are independent. That’s why certain DirectX calls can be in the end simple wrappers around memcpy(-like).  
  
of course this is still a lot simplified description, but I hope it suffices and is clear.
  -  NB  
LB March 21, 2025  
I guess some data is better kept in the client process. Perhaps this is why the Vulkan API lets you provide an allocator for the driver to use.

## Stay informed

---

Get notified when new posts are published.