X86 Attack Vector Controls

SEPTEMBER 2024

LINUX PLUMBERS – X86 MICROCONFERENCE

[Public]

ATTACK VECTOR CONTROLS

- **Problem:** bugs.c tries to mitigate ~15 CPU speculation bugs. Few people understand these bugs and when to worry about them.
- ***Attack vector controls*** configure mitigations based on how a system will be used
  - ***mitigate_user_kernel=<on/off>***
    - Disable if no untrusted userspace is being run, such as single-user systems
  - ***mitigate_user_user =<on/off>***
    - Disable if no untrusted userspace is being run
  - ***mitigate_guest_host =<on/off>***
    - Disable if no untrusted VMs are being run
  - ***mitigate_guest_guest =<on/off>***
    - Disable if no untrusted VMs, or only single VM
  - ***mitigate_cross_thread =<on/off>***
    - Enable if untrusted code may run on sibling threads

Vulnerability	User-to-Kernel	User-to-User	Guest-to-Host	Guest-to-Guest	Cross-Thread
BHI	X		X		
GDS	X	X	X	X	
L1TF			X		*
MDS	X	X	X	X	*
MMIO	X	X	X	X	*
Meltdown	X				
Retbleed	X		X		*
RFDS	X	X	X	X	
Spectre_v1	X				
Spectre_v2	X		X		
Spectre_v2_user		X		X	
SRBDS	X	X	X	X	
SRSO	X		X		
SSB					
TAA	X	X	X	X	*

* Disables SMT if required

- Attack vector controls may be overridden by individual bug controls or ***mitigations=off***

[Public]

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. The information contained herein is subject to change and may be rendered inaccurate for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product releases, product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. Any computer system has risks of security vulnerabilities that cannot be completely prevented or mitigated. AMD assumes no obligation to update or otherwise correct or revise this information. However, AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

THIS INFORMATION IS PROVIDED ‘AS IS.” AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND ASSUMES NO RESPONSIBILITY FOR ANY INACCURACIES, ERRORS, OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION. AMD SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AMD BE LIABLE TO ANY PERSON FOR ANY RELIANCE, DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF AMD IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AMD, the AMD Arrow logo, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

© 2024 Advanced Micro Devices, Inc. All rights reserved.