

Intel will stop releasing patches for the Specter v2 security hole on some older CPUs

Recently, Intel has confirmed that it will stop updating the Meltdown and Specter security patches for certain products.

Recently, Intel has confirmed that it will stop updating the Meltdown and Specter security patches for certain products. No more microcode patches will be released in the future because the process of removing Specter v2 is too complicated and contains many risks.

In the microcode test guide, Intel said that after conducting a thorough check of microcode microstructures and performance on CPUs with a similar structure and patch that is no longer widely used, available on the market today (launched from about 10 years ago (2007-2011)), they made this decision.



If a particular processor falls into one of the following three categories, it will be on the list of receiving 'stop' confirmations in the new Intel documentation.

1. Microstructure features on these CPUs tend to conflict and prevent some microcode features to overcome Specter v2 vulnerability (CVE-2017-5715).
2. Current microcode updates are still quite limited in the ability to support commercial software systems.
3. Most of these hardware products are closed systems, so the ability to 'stick' these security holes is quite low.

This list includes processors like Bloomfield, Bloomfield Xeon, Clarksfield, Gulftown, Harpentown Xeon C0 and E0, Jasper Forest, Penryn / QC, SoFIA 3GR, Wolfdale, Wolfdale Xeon, Yorkfield, Yorkfield Xeon and many other names Xeon, Core CPU, Pentium, Celeron and Atom series.



Currently, Intel is also implementing a number of measures to overcome security holes on some chips that have not received any previous updates such as Arrandale, Clarkdale, Lynnfield, Nehalem and Westmere.

See more:

1. Intel faces a new vulnerability called BranchScope
2. The new Specter vulnerability appears to be a new variant that easily 'crashes' secure partitions created by Intel SGX
3. Intel released a new patch to fix the Specter and Meltdown vulnerabilities

You finished reading the article "**Intel will stop releasing patches for the Specter v2 security hole on some older CPUs**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.