



# Download

[Update To Disable Mitigation Against Spectre, Variant 2](#)

Microsoft Support

## Update to disable mitigation against Spectre, Variant 2

Email

Print

Applies to: [Windows 7 Service Pack 1](#), [Windows 8.1](#), [Windows 10](#), [More](#)

### Summary

Intel has reported issues with recently released microcode meant to address Spectre variant 2 (CVE 2017-5715 Branch Target Injection) – specifically Intel noted that this microcode can cause “higher than expected reboots and other unpredictable system behavior” and then noted that situations like this may result in “data loss or corruption.” Our own experience is that system instability can in some circumstances cause data loss or corruption. On January 22, Intel recommended that customers stop deploying the current microcode version on affected processors while they perform additional testing on the updated solution. We understand that Intel is continuing to investigate the potential effect of the current microcode version, and we encourage customers to review their guidance on an ongoing basis to inform their decisions.

While Intel tests, updates and deploys new microcode, we are making available an out-of-band update today, KB4078130, that specifically disables only the mitigation against CVE 2017-5715 – “Branch target injection vulnerability.” In our testing, this update has been found to prevent the described behavior in devices that have affected microcode. For the full list of affected devices, see [Intel’s microcode revision guidance](#). This update covers Windows 7 (SP1), Windows 8.1, and all versions of Windows 10, for client and server. If you are running an affected device, this update can be applied by downloading it from the [Microsoft Update Catalog website](#). Application of this payload specifically disables only the mitigation against CVE-2017-5715 – “Branch target injection vulnerability.”

**Note** Users who do not have the affected Intel microcode do not have to download this update.

Site feedback

[Update To Disable Mitigation Against Spectre, Variant 2](#)



**Download**

---

... Intel's fix and Microsoft is also offering an option for advanced users "to manually disable and enable the mitigation against Spectre variant 2 .... The "Update to Disable Mitigation against Spectre, Variant 2" should only be installed if you're "running an impacted device" the software giant .... Microsoft Issues Emergency Patch to Disable Intel's Broken Spectre Fix ... specifically disables only the mitigation against CVE-2017-5715," Microsoft said. ... This does mean that Spectre Variant 2 is not mitigated, but there are ...

... Windows Update to Disable Mitigation Against Spectre Variant 2 ... The out-of-band update, KB4078130, is meant for Windows 7 (SP1), ...

[Bet canl bein sport](#)

Just after the release of the Meltdown and Spectre security updates Intel excluded ... that specifically disables only the mitigation against CVE-2017-5715 ... and disable Spectre Variant 2 mitigations through registry settings.. Microsoft Releases Windows Update To Disable Intel's Flawed Spectre Mitigation. ... address Spectre variant 2 (CVE 2017-5715 Branch Target Injection). ... that specifically disables only the mitigation against CVE-2017-5715 .... Microsoft releases another security patch against 'Spectre Variant 2' ... to manually disable and enable the mitigation against Spectre Variant 2 .... A patch for Spectre Variant 2 listed as CVE-2017-5715 was released. ... with our vendors to deploy the required updates to mitigate vulnerabilities. ... around the clock to have our infrastructure patched against the Meltdown and Spectre ... Disabling this cookie will limit you from receiving assistance from the ... [iPhone 7 Stuck in "Headphone" Mode – How to Fix](#)

Microsoft Support

## Update to disable mitigation against Spectre, Variant 2

Email

Print

Applies to: [Windows 7 Service Pack 1](#), [Windows 8.1](#), [Windows 10](#); [More](#)

### Summary

Intel has reported issues with recently released microcode meant to address Spectre variant 2 (CVE 2017-5715 Branch Target Injection) – specifically Intel noted that this microcode can cause "higher than expected reboots and other unpredictable system behavior" and then noted that situations like this may result in "data loss or corruption." Our own experience is that system instability can in some circumstances cause data loss or corruption. On January 22, Intel recommended that customers **stop deploying the current microcode version** on affected processors while they perform additional testing on the updated solution. We understand that Intel is continuing to investigate the potential effect of the current microcode version, and we encourage customers to review their guidance on an ongoing basis to inform their decisions.

While Intel tests, updates and deploys new microcode, we are making available an out-of-band update today, KB4078130, that specifically disables only the mitigation against CVE-2017-5715 – "Branch target injection vulnerability." In our testing, this update has been found to prevent the described behavior in devices that have affected microcode. For the full list of affected devices, see [Intel's microcode revision guidance](#). This update covers Windows 7 (SP1), Windows 8.1, and all versions of Windows 10, for client and server. If you are running an affected device, this update can be applied by downloading it from the [Microsoft Update Catalog website](#). Application of this payload specifically disables only the mitigation against CVE-2017-5715 – "Branch target injection vulnerability."

**Note** Users who do not have the affected Intel microcode do not have to download this update.

Site feedback

[BGR scoops up](#)

---

[Verizon roadmap, Droids, Tablets, LTE, and more](#)

[Facebook Reunions: Balzer Sisters Reunite](#)

“Update to Disable Mitigation against Spectre, Variant 2” in Windows – out of band update released <https://t.co/YxAiHd2z4l>. — Kevin Beaumont .... In order to mitigate the Spectre vulnerabilities in Windows 10, ... Microsoft has updated their article to indicate that the above Registry ... In particular, for Server SKUs, these settings will enable Spectre variant 2 mitigations ... will i get problem for enabling retpoline in my pc? and if so, how do i disable it?. ... purpose of this advisory is to bring attention to a recently released Microsoft Security Update to Disable Mitigation against Spectre, Variant 2.. This update enables the “Retpoline” mitigation that addresses the Spectre variant 2 (CVE-2017-5715) vulnerability. Retpoline was developed by Google's Project Zero team, to increase protection against “branch target injection” attacks, ... on to a Windows Server system and disable multiple RDP sessions.. IT admins can also manually disable Intel's mitigation against Spectre Variant 2 by applying new registry key settings, and more details are ... ([iPhone](#), [iPad](#))

[1208 Pm Files Free Download](#)

Microsoft has released another security patch against 'Spectre Variant 2' bug found on Intel chips. Microsoft has released another security update to address the .... Scripts downloads and runs Microsoft's KB4078130 patch. This script disables Intel Microcode meant to mitigate against Spectre variant 2. Machines running this .... For Windows users, Microsoft now offers a patch that reverses Intel's ... Update to disable mitigation against Spectre, Variant 2 [Microsoft, via .... ... security patch against 'Spectre Variant 2' bug found on Intel chips. ... to manually disable and enable the mitigation against Spectre Variant 2 .... For further information on enabling or disabling the mitigation, consult 'Disable mitigation against Spectre variant 2 independently' on Microsoft: .... ... Windows update that disables patches for the Spectre Variant 2 bug ... manually disable and enable the mitigation against Spectre Variant 2 .... Spectre is a vulnerability that affects modern microprocessors that perform branch prediction. ... "Update to Disable Mitigation against Spectre, Variant 2". 82abd11c16 [Origin 10.5.63 Crack with Keys Free Download 2020](#)

82abd11c16

[Cisdem Video Converter 4.10 Full macOS](#)  
[Filterloop Pro v2.4.1 \[All Filters Unlocked\] \[Latest\]](#)  
[\[Movie\] Behind Enemy Lines \(BLURAY\)](#)