What to do to protect the device from ZombieLoad attack?

Recently a new vulnerability was found on Intel processor chip called ZombieLoad that made users worried. If you are looking for ways to protect your device, then you are in the right place.

Recently a new vulnerability was found on Intel processor chip called ZombieLoad that made users worried. If you are looking for ways to protect your device, then you are in the right place. This article will give you all the information you need to make sure the device is protected against this attack.

ZombieLoad affects Intel processors manufactured since 2011, so if there's a device using this Intel processor, read on to learn how to protect it. Recently, AMD officially confirmed that their processor is not affected by ZombieLoad, so it seems that it is still the only flaw of Intel.

1. Which company CPU should I choose: Intel or AMD?

If you are worried that your device has been hacked, you need to make sure you have all the latest patches and updates available for your operating system.

How to protect the device from ZombieLoad security holes

1. So what is ZombieLoad?
2. How to check equipment affected by ZombieLoad vulnerability
3. How to protect against ZombieLoad CPU security holes
    1. How to fight ZombieLoad CPU vulnerability on Android device
    2. How to combat ZombieLoad CPU security holes on Windows computers
    3. How to fix the ZombieLoad CPU security hole on a Mac
    4. How to fix the ZombieLoad CPU security hole on Linux
    5. How to fix ZombieLoad vulnerability on Chromebook
    6. How to protect Firefox and Chrome before ZombieLoad

So what is ZombieLoad?

ZombieLoad is a security vulnerability that allows hackers to steal private browsing history, passwords and other information from affected computers using software that exploits an error in Intel's hardware.

ZombieLoad is also called CVE-2018-12130, it uses vulnerabilities in the way the CPU handles load zombies, this is a large amount of data that the processor cannot handle properly, making it use microcode (A script inside

the CPU to describe the commands to be executed) to prevent a problem. This vulnerability allows access to sensitive data from programs and applications.

How to check equipment affected by ZombieLoad vulnerability

Unfortunately, there is currently no way to check if your device is affected by the ZombieLoad vulnerability. And anti-virus software, Internet security suites cannot detect this vulnerability. However, if you use an Intel-powered device manufactured in 2011, it is likely that your device will be attacked by ZombieLoad.

Devices such as Windows, Mac, Intel-based tablets can all be hacked, unless you use devices running on AMD or ARM processors. However, you do not need to be too frightened when using devices running Intel processors because this only proves that the device is more vulnerable to attack and is not sure that it has been targeted. You just need to make sure your devices are updated to protect against ZombieLoad as soon as possible.

How to protect against ZombieLoad CPU security holes

Here are the measures to overcome and protect the security hole ZombieLoad CPU on different devices.

How to fight ZombieLoad CPU vulnerability on Android device

Although most Android devices run ARM hardware and are not affected by ZombieLoad, other Android devices that use Intel need to update the patches.

These patches are provided by Android device hardware manufacturers, not from Google, so you need to visit the manufacturer's website or contact them directly to receive a patch when delivered. onions.

You can also check for updates yourself by opening the settings on your Android device, accessing the **System** and seeing if there are new updates.

How to combat ZombieLoad CPU security holes on Windows computers

Windows computers and laptops are most likely to be attacked by ZombieLoad because most of these devices run on Intel hardware. This vulnerability affects Windows 7, Windows XP and Windows 10 computers.

The good news is that Microsoft has released security updates for Windows 10 as well as previous Windows versions. Windows 10 will automatically download the update, but to be sure you can type **windows update** in the search bar on the Taskbar and select **Check for updates** . If there is an update, download and install it on the system. Also you can download the fix for ZombieLoad from Microsoft Support website.

How to fix the ZombieLoad CPU security hole on a Mac

The Mac is also affected by ZombieLoad and it has released the ZombieLoad patch for macOS Mojave 10.14.5, applicable to all Macs and MacBooks released since 2011. This patch also includes an update for the program. Browse Internet Safari.

However, it seems that some Macs lose 40% performance if all of these patches are applied. Hope Apple and Intel can work together to minimize the impact on performance.

In addition, there is an update for Mac running macOS Sierra and macOS High Sierra. iPhone and iPad are not affected by this vulnerability.

For older macOS versions, pay attention to the Mac App Store to see if there are any new updates for OS X or macOS to ensure the device runs the latest version on the operating system.

How to fix the ZombieLoad CPU security hole on Linux

ZombieLoad also affects Linux machines running on Intel hardware. Greg Kroah-Hartman, a stable Linux kernel maintenance, announced the release of the Linux kernel 5.1.2. Meanwhile, development distro teams also release fixes. Red Hat has announced that Red Hat Enterprise Linux (RHEL) 5 to the latest version of RHEL 8 is also affected by this vulnerability, as well as Red Hat Virtualization and Red Hat OpenStack.

Red Hat has developed kernel security updates for their products, so make sure you have installed the latest updates. However, these patches can lead to performance issues.

Canonical, the company behind the famous Linux Linux distribution, has also released information on how to fight ZombieLoad.

How to fix ZombieLoad vulnerability on Chromebook

If using Chromebook, you will be protected automatically from ZombieLoad, because Chrome OS will automatically update and the latest version - Chrome OS 74, disable Hyper-Threading to prevent ZombieLoad vulnerability.

This may impact performance, but Google is trying to add measures against ZombieLoad to Chrome OS 75.

How to protect Firefox and Chrome before ZombieLoad

Mozilla also said it is studying a long-term fix for the MacOS Firefox web browser and has a patch for Firefox and Firefox Nightly versions. According to Mozilla, they do not need to take any action for Firefox users on

Windows and Linux.

If you use Google's Chrome web browser, Google recommends that you make sure the operating system it runs (probably Windows, Linux or macOS) is updated to the latest version.

I wish you all success!