Linux Mint / Ubuntu: Meltdown and Spectre

Security updates are now available for Meltdown and Spectre.

> Meltdown and Spectre exploit critical vulnerabilities in modern . These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.
>
> Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

If you haven't already done so, please read "Meltdown and Spectre".

These vulnerabilities are critical. They expose all memory data present on the computer to any application running locally (including to scripts run by your web browser).

Note: Meltdown and Spectre also affect smart phones and tablets. Please seek information on how to protect your mobile devices.

Firefox 57.0.4

Firefox was patched. Please use the Update Manager to upgrade it to version to 57.0.4.

https://usn.ubuntu.com/usn/usn-3516-1/

https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

NVIDIA 384.111

If you are using the NVIDIA proprietary drivers, upgrade them to version 384.111.

In Linux Mint 17.x and 18.x, this update is available in the Update Manager.

In LMDE, it is available on the NVIDIA Website.

https://forums.geforce.com/default/topic/1033210/nvidias-response-to-speculative-side-channels-cve-2017-5753-cve-2017-5715-and-cve-2017-5754/

https://usn.ubuntu.com/usn/usn-3521-1/

Chrome Site Isolation

If you are using Google Chrome or Chromium, please follow the steps below:

- Type **chrome://flags** in the address bar and press **Enter**.
- Scroll down the page and find "**Strict site isolation**" and press the **Enable** button.
- Restart the Chrome browser.

https://www.chromium.org/Home/chromium-security/ssca

Opera

If you are using the Opera browser, visit opera://flags/?search=enable-site-per-process, click **Enable** and restart Opera.

Linux Kernel 3.16.51-3+deb8u1 (LMDE)

If you are using LMDE, please use the Update Manager to upgrade your Linux kernel to version 3.16.51-3+deb8u1.

https://security-tracker.debian.org/tracker/CVE-2017-5754

Linux Kernel (Linux Mint 17.x)

Please stay tuned for a kernel update in Linux Mint 17.x.

https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown

Linux Kernel (Linux Mint 18.x)

Please stay tuned for a kernel update in Linux Mint 18.x.

https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown

Other Updates

Other updates should become available in the near future, including but not limited to qemu and CPU microcode.

General Advice

Locally, you should backup your personal data and set up daily system snapshots (timeshift is recommended for that).

Apply security updates as they become available on all your devices.

Review any sensitive information stored online.

Stay away from 3rd party applications, proprietary in particular and do not visit websites you don’t trust on devices which haven’t been patched.

Consider securing access to your important data (your email account in particular) with 2 factor authentication.