Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Today's CPU vulnerability: what you need to know

January 3, 2018

Posted by Matt Linton, Senior Security Engineer and Pat Parseghian, Technical Program Manager

[Google Cloud, G Suite, and Chrome customers can visit the Google Cloud blog for details about those products]
[For more technical details about this issue, please read Project Zero's blog post]

Last year, Google's Project Zero team discovered serious security flaws caused by "speculative execution," a technique used by most modern processors (CPUs) to optimize performance.

The Project Zero researcher, Jann Horn, demonstrated that malicious actors could take advantage of speculative execution to read system memory that should have been inaccessible. For example, an unauthorized party may read sensitive information in the system's memory such as passwords, encryption keys, or sensitive information open in applications. Testing also showed that an attack running on one virtual machine was able to access the physical memory of the host machine, and through that, gain read-access to the memory of a different virtual machine on the same host.

These vulnerabilities affect many CPUs, including those from AMD, ARM, and Intel, as well as the devices and operating systems running on them.

As soon as we learned of this new class of attack, our security and product development teams mobilized to defend Google's systems and our users' data. We have updated our systems and affected products to protect against this new type of attack. We also collaborated with hardware and software manufacturers across the industry to help protect their users and the broader web. These efforts have

included collaborative analysis and the development of novel mitigations.

We are posting before an originally coordinated disclosure date of January 9, 2018 because of existing public reports and growing speculation in the press and security research community about the issue, which raises the risk of exploitation. The full Project Zero report is forthcoming (update: this has been published; see above).

Mitigation status for Google products

A list of affected Google products and their current status of mitigation against this attack appears here. As this is a new class of attack, our patch status refers to our mitigation for currently known vectors for exploiting the flaw. The issue has been mitigated in many products (or wasn't a vulnerability in the first place). In some instances, users and customers may need to take additional steps to ensure they're using a protected version of a product. This list and a product's status may change as new developments warrant. In the case of new developments, we will post updates to this blog.

- All Google products not explicitly listed below require no user or customer action.
- Android
    - Devices with the latest security update are protected. Furthermore, we are unaware of any successful reproduction of this vulnerability that would allow unauthorized information disclosure on ARM-based Android devices.

    - Supported Nexus and Pixel devices with the latest security update are protected.
    - Further information is available here.

- Google Apps / G Suite (Gmail, Calendar, Drive, Sites, etc.):
    - No additional user or customer action needed.
- Google Chrome
    - Some user or customer action needed. More information here.
- Google Chrome OS (e.g., Chromebooks):
    - Some additional user or customer action needed. More information here.
- Google Cloud Platform
    - Google App Engine: No additional customer action needed.
    - Google Compute Engine: Some additional customer action needed. More information here.
    - Google Kubernetes Engine: Some additional customer action needed. More information here.
    - Google Cloud Dataflow: Some additional customer action needed. More information here.
    - Google Cloud Dataproc: Some additional customer action needed. More information here.
    - All other Google Cloud products and services: No additional action needed.
- Google Home / Chromecast:

    - No additional user action needed.

- Google Wifi/OnHub:

    - No additional user action needed.

Multiple methods of attack

To take advantage of this vulnerability, an attacker first must be able to run malicious code on the targeted system.

The Project Zero researchers discovered three methods (variants) of attack, which are effective under different conditions. All three attack variants can allow a process with normal user privileges to perform unauthorized reads of memory data, which may contain sensitive information such as passwords, cryptographic key material, etc.

In order to improve performance, many CPUs may choose to speculatively execute instructions based on assumptions that are considered likely to be true. During speculative execution, the processor is verifying these assumptions; if they are valid, then the execution continues. If they are invalid, then the execution is unwound, and the correct execution path can be started based on the actual conditions. It is possible for this speculative execution to have side effects which are not restored when the CPU state is unwound, and can lead to information disclosure.

There is no single fix for all three attack variants; each requires protection independently. Many vendors have patches available for one or more of these attacks.

We will continue our work to mitigate these vulnerabilities and will update both our product support page and this blog post as we release further fixes. More broadly,

we appreciate the support and involvement of all the partners and Google engineers who worked tirelessly over the last few months to make our users and customers safe.

Blog post update log

- Added link to Project Zero blog
- Added link to Google Cloud blog

No comments :

Post a Comment