# Meltdown and Spectre

Vulnerabilities in modern computers leak passwords and sensitive data.

Meltdown and Spectre exploit critical vulnerabilities in modern processors (The main part of every computer). 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.

# Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information. This applies both to personal computers as well as cloud infrastructure. Luckily, there are software patches against Meltdown.

Meltdown Paper

Cite

arXiv

# Spectre

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre

Spectre is harder to exploit than Meltdown, but it is also harder to mitigate. However, it is possible to prevent specific known exploits based on Spectre through software patches.

Spectre Paper

Cite

arXiv

## Who reported Meltdown?

Meltdown was independently discovered and reported by three teams:

- Jann Horn (Google Project Zero),
- Werner Haas, Thomas Prescher (Cyberus Technology),
- Daniel Gruss, Moritz Lipp, Stefan Mangard, Michael Schwarz (Graz University of Technology)

## Who reported Spectre?

Spectre was independently discovered and reported by two people:

- Jann Horn (Google Project Zero) and
- Paul Kocher in collaboration with, in alphabetical order, Daniel Genkin (University of Pennsylvania and University of Maryland), Mike Hamburg (Rambus), Moritz Lipp (Graz University of Technology), and Yuval Yarom (University of Adelaide and Data61)

---

## Questions & Answers

### Am I affected by the vulnerability?

Most certainly, yes.

### Can I detect if someone has exploited Meltdown or Spectre against me?

Probably not. The exploitation does not leave any traces in traditional log files.

### Can my antivirus detect or block this attack?

While possible in theory, this is unlikely in practice. Unlike usual malware, Meltdown and Spectre are hard to distinguish from regular benign applications. However, your antivirus may detect malware which uses the attacks by comparing binaries after they become known.

### What can be leaked?

If your system is affected, our proof-of-concept exploit can read the memory content of your computer. This may include passwords and sensitive data stored on the system.

### Has Meltdown or Spectre been abused in the wild?

We don't know.

### Is there a workaround/fix?

There are patches against Meltdown for Linux ( KPTI (formerly KAISER)), Windows, and OS X. There is also work to harden software against future exploitation of Spectre, respectively to patch software after exploitation through Spectre ( LLVM patch, MSVC, ARM speculation barrier header).

### Which systems are affected by Meltdown?

Desktop, Laptop, and Cloud computers may be affected by Meltdown. More technically, every Intel processor which implements out-of-order execution is potentially affected, which is effectively every processor since 1995 (except Intel Itanium and Intel Atom before 2013). We successfully tested Meltdown on Intel processor generations released as early as 2011. Currently, we have only verified Meltdown on Intel processors. At the moment, it is unclear whether AMD processors are also affected by Meltdown. According to ARM, some of their processors are also affected.

### Which systems are affected by Spectre?

Almost every system is affected by Spectre: Desktops, Laptops, Cloud Servers, as well as Smartphones. More specifically, all modern processors capable of keeping many instructions in

flight are potentially vulnerable. In particular, we have verified Spectre on Intel, AMD, and ARM processors.

### Which cloud providers are affected by Meltdown?

Cloud providers which use Intel CPUs and Xen PV (Xen paravirtualization) as virtualization without having patches applied. Furthermore, cloud providers without real hardware virtualization, relying on containers that share one kernel, such as Docker, LXC, or OpenVZ are affected.

### What is the difference between Meltdown and Spectre?

Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory. Consequently, applications can access system memory. Spectre tricks other applications into accessing arbitrary locations in their memory. Both attacks use side channels to obtain the information from the accessed memory location. For a more technical discussion we refer to the papers ( Meltdown and Spectre)

### Why is it called Meltdown?

The vulnerability basically melts security boundaries which are normally enforced by the hardware.

### Why is it called Spectre?

The name is based on the root cause, speculative execution. As it is not easy to fix, it will haunt us for quite some time.

### Is there more technical information about Meltdown and Spectre?

Yes, there is an academic paper and a blog post about Meltdown, and an academic paper about Spectre. Furthermore, there is a Google Project Zero blog entry about both attacks.

### What are CVE-2017-5753 and CVE-2017-5715?

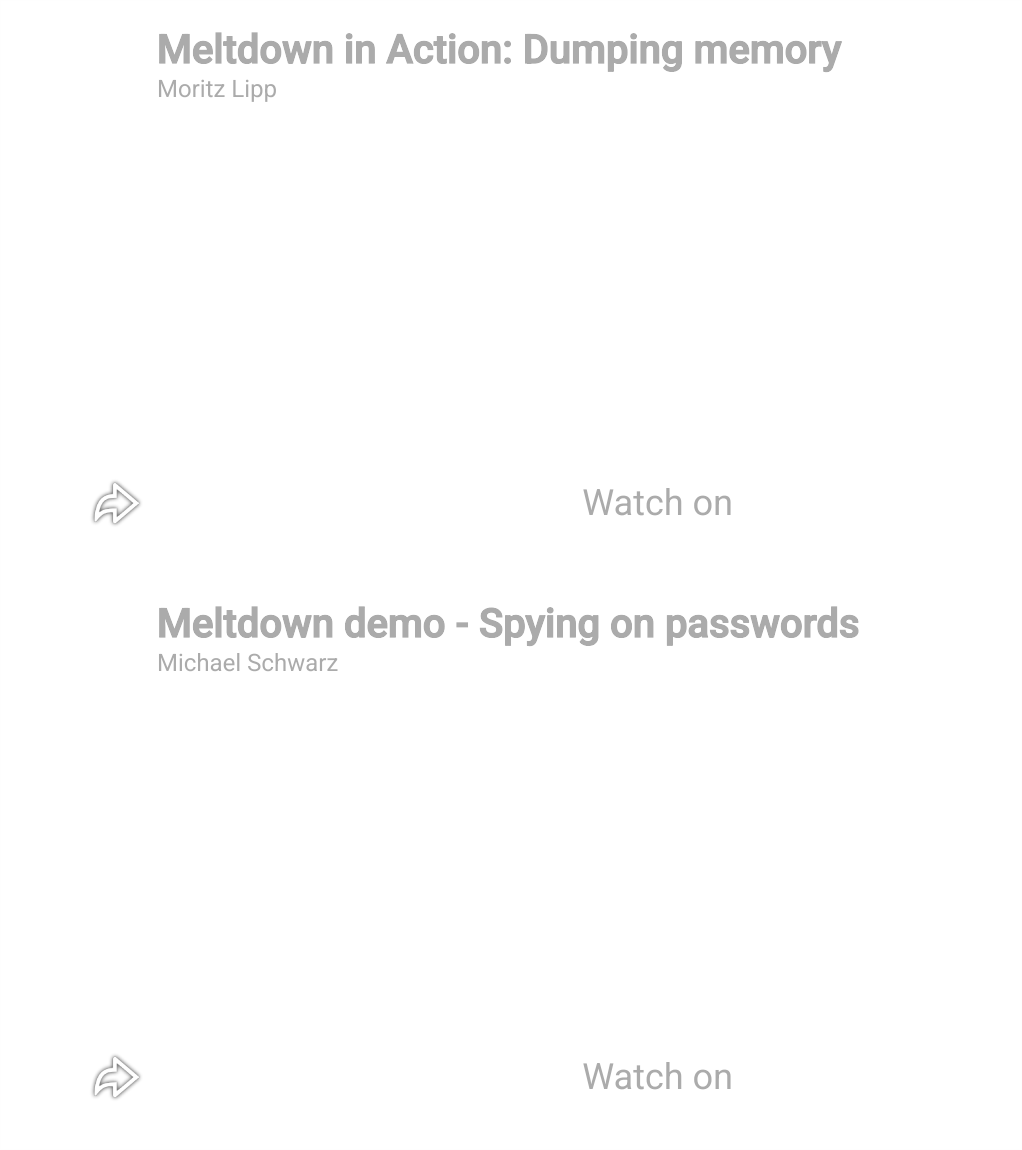
CVE-2017-5753 and CVE-2017-5715 are the official references to Spectre. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names

maintained by MITRE.

### What is the CVE-2017-5754?

CVE-2017-5754 is the official reference to Meltdown. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE.

### Can I see Meltdown in action?



**Reconstructing images with Meltdown**
Moritz Lipp

Watch on

**Reconstructing a photo with Meltdown**
Michael Schwarz

Watch on

### Can I use the logo?

Both the Meltdown and Spectre logo are free to use, rights waived via CC0. Logos are designed by Natascha Eibl.

| | Logo | Logo with text | Code illustration |
|---|---|---|---|
| **Meltdown** | PNG / SVG | PNG / SVG | PNG / SVG |
| **Spectre** | PNG / SVG | PNG / SVG | PNG / SVG |

### Is there a proof-of-concept code?

Yes, there is a GitHub repository containing test code for Meltdown.

### Where can I find official infos/security advisories of involved/affected companies?

| | Link |
|---|---|
| **Intel** | Security Advisory / Newsroom / Whitepaper |
| **ARM** | Security Update |
| **AMD** | Security Information |
| **RISC-V** | Blog |
| **NVIDIA** | Security Bulletin / Product Security |
| **Microsoft** | Security Guidance / Information regarding anti-virus software / Azure Blog / Windows (Client) / Windows (Server) |
| **Amazon** | Security Bulletin |
| **Google** | Project Zero Blog / Need to know |
| **Android** | Security Bulletin |
| **Apple** | Apple Support |
| **Lenovo** | Security Advisory |
| **IBM** | Blog |
| **Dell** | Knowledge Base / Knowledge Base (Server) |
| **Hewlett Packard Enterprise** | Vulnerability Alert |
| **HP Inc.** | Security Bulletin |
| **Huawei** | Security Notice |
| **Synology** | Security Advisory |
| **Cisco** | Security Advisory |

| | |
|---|---|
| **F5** | Security Advisory |
| **Mozilla** | Security Blog |
| **Red Hat** | Vulnerability Response / Performance Impacts |
| **Debian** | Security Tracker |
| **Ubuntu** | Knowledge Base |
| **SUSE** | Vulnerability Response |
| **Fedora** | Kernel update |
| **Qubes** | Announcement |
| **Fortinet** | Advisory |
| **NetApp** | Advisory |
| **LLVM** | Spectre (Variant #2) Patch / Review __builtin_load_no_speculate / Review llvm.nospeculateload |
| **CERT** | Vulnerability Note |
| **MITRE** | CVE-2017-5715 / CVE-2017-5753 / CVE-2017-5754 |
| **VMWare** | Security Advisory / Blog |
| **Citrix** | Security Bulletin / Security Bulletin (XenServer) |
| **Xen** | Security Advisory (XSA-254) / FAQ |

### Acknowledgements

We would like to thank Intel for awarding us with a bug bounty for the responsible disclosure process, and their professional handling of this issue through communicating a clear timeline and connecting all involved researchers. Furthermore, we would also thank ARM for their fast response upon disclosing the issue.

This work was supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 681402).

This work was supported in part by NSF awards #1514261 and #1652259, financial assistance award 70NANB15H328 from the U.S. Department of Commerce, National Institute of Standards and Technology, the 2017-2018 Rothschild Postdoctoral Fellowship, and the Defense Advanced Research Project Agency (DARPA) under Contract #FA8650-16-C-7622.