Hertzbleed Attack

Paper Q&A

Hertzbleed is a new family of side-channel attacks: frequency side channels. In the worst case, these attacks can allow an attacker to extract cryptographic keys from remote servers that were previously believed to be secure.

Hertzbleed takes advantage of our experiments showing that, under certain circumstances, the dynamic frequency scaling of modern x86 processors depends on the data being processed. This means that, on modern processors, the same program can run at a different CPU frequency (and therefore take a different wall time) when computing, for example, `2022 + 23823` compared to `2022 + 24436`.

Hertzbleed is a real, and practical, threat to the security of cryptographic software. We have demonstrated how a clever attacker can use a novel chosen-ciphertext attack against SIKE to perform full key extraction via remote timing, despite SIKE being implemented as "constant time".

Research Paper

The Hertzbleed paper will appear in the 31st USENIX Security Symposium (Boston, 10–12 August 2022) with the following title:

- *Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86*

You can download a preprint from here.

The paper is the result of a collaboration between the following researchers:

- Yingchen Wang (University of Texas at Austin)
- Riccardo Paccagnella (University of Illinois Urbana-Champaign)
- Elizabeth Tang He (University of Illinois Urbana-Champaign)
- Hovav Shacham (University of Texas at Austin)
- Christopher Fletcher (University of Illinois Urbana-Champaign)
- David Kohlbrenner (University of Washington)

Questions and Answers

Am I affected by Hertzbleed?

Likely, yes.

Intel's security advisory states that *all* Intel processors are affected. We experimentally confirmed that several Intel processors are affected, including desktop and laptop

models from the 8th to the 11th generation Core microarchitecture.

AMD's security advisory states that several of their desktop, mobile and server processors are affected. We experimentally confirmed that AMD Ryzen processors are affected, including desktop and laptop models from the Zen 2 and Zen 3 microarchitectures.

Other processor vendors (e.g., ARM) also implement frequency scaling in their products and were made aware of Hertzbleed. However, we have not confirmed if they are, or are not, affected by Hertzbleed.

What is the impact of Hertzbleed?

First, Hertzbleed shows that on modern x86 CPUs, power side-channel attacks can be turned into (even remote!) timing attacks—lifting the need for any power measurement interface. The cause is that, under certain circumstances, periodic CPU frequency adjustments depend on the current CPU power consumption, and these adjustments directly translate to execution time differences (as 1 hertz = 1 cycle per second).

Second, Hertzbleed shows that, even when implemented correctly as constant time, cryptographic code can still leak via remote timing analysis. The result is that current industry guidelines for how to write constant-time code (such as Intel's one) are insufficient to guarantee constant-time execution on modern processors.

Is there an assigned CVE for Hertzbleed?

Yes. Hertzbleed is tracked under CVE-2022-23823 and CVE-2022-24436 in the Common Vulnerabilities and Exposures (CVE) system.

Is Hertzbleed a bug?

No. The root cause of Hertzbleed is dynamic frequency scaling, a *feature* of modern processors, used to reduce power consumption (during low CPU loads) and to ensure that the system stays below power and thermal limits (during high CPU loads).

When did you disclose Hertzbleed?

We disclosed our findings, together with proof-of-concept code, to Intel, Cloudflare and Microsoft in Q3 2021 and to AMD in Q1 2022. Intel originally requested our findings be held under embargo until May 10, 2022. Later, Intel requested a significant extension of that embargo, and we coordinated with them on publicly disclosing our findings on June 14, 2022.

Do Intel and AMD plan to release microcode patches to mitigate Hertzbleed?

No. To our knowledge, Intel and AMD do not plan to deploy any microcode patches to mitigate Hertzbleed. However, Intel provides guidance to mitigate Hertzbleed in software. Cryptographic developers may choose to follow Intel's guidance to harden their libraries and applications against Hertzbleed. For more information, we refer to the official security advisories (Intel and AMD).

Why did Intel ask for a long embargo, considering they are not deploying patches?

Ask Intel.

Is there a workaround?

Technically, yes. However, it has an extreme system-wide performance impact.

You can prevent Hertzbleed by disabling frequency boost. Intel calls this feature "Turbo Boost", and AMD calls it "Turbo Core" or "Precision Boost". Disabling frequency boost can be done either through the BIOS or at runtime via the frequency scaling driver. When frequency boost is disabled, the frequency stays fixed at the base frequency during workload execution, preventing leakage via Hertzbleed. This is not a recommended mitigation strategy as it will very significantly impact performance.

What is SIKE?

SIKE (Supersingular Isogeny Key Encapsulation) is a decade old, widely studied key encapsulation mechanism. It is currently a finalist in NIST's Post-Quantum Cryptography competition. It has multiple industrial implementations and was the subject of an in-the-wild deployment experiment. Among its claimed advantages are a "well-understood" side channel posture. You can find author names, implementations, talks, studies, articles, security analyses and more about SIKE on its official website.

What is a key encapsulation mechanism?

A key encapsulation mechanism is a protocol used to securely exchange a symmetric key using asymmetric (public-key) cryptography.

How did Cloudflare and Microsoft mitigate the attack on SIKE?

Both Cloudflare and Microsoft deployed the mitigation suggested by De Feo et al. (who, while our paper was under the long Intel embargo, independently re-discovered how to exploit anomalous 0s in SIKE for power side channels). The mitigation consists of validating, before decapsulation, that the ciphertext consists of a pair of linearly independent points of the correct order. The mitigation adds a decapsulation performance overhead of 5% for CIRCL and of 11% for PQCrypto-SIDH.

Is my constant-time cryptographic library affected?

Affected? Likely yes. Vulnerable? Maybe.

Your constant-time cryptographic library might be vulnerable if is susceptible to secret-dependent power leakage, and this leakage extends to enough operations to induce secret-dependent changes in CPU frequency. Future work is needed to systematically study what cryptosystems can be exploited via the new Hertzbleed side channel.

Can I use the logo?

Yes. The Hertzbleed logo is free to use under a CC0 license.

- Download logo: SVG, PNG
- Download logo with text: SVG, PNG

Did we really need another vulnerability logo?

We know some of you don't really like vulnerability logos, and we hear you. However, we really like our logo (and hope you do too!).

Did you release the source code of the Hertzbleed attack?

Yes, for full reproducibility. You can find the source code of all the experiments from our paper at the link: https://github.com/FPSG-UIUC/hertzbleed