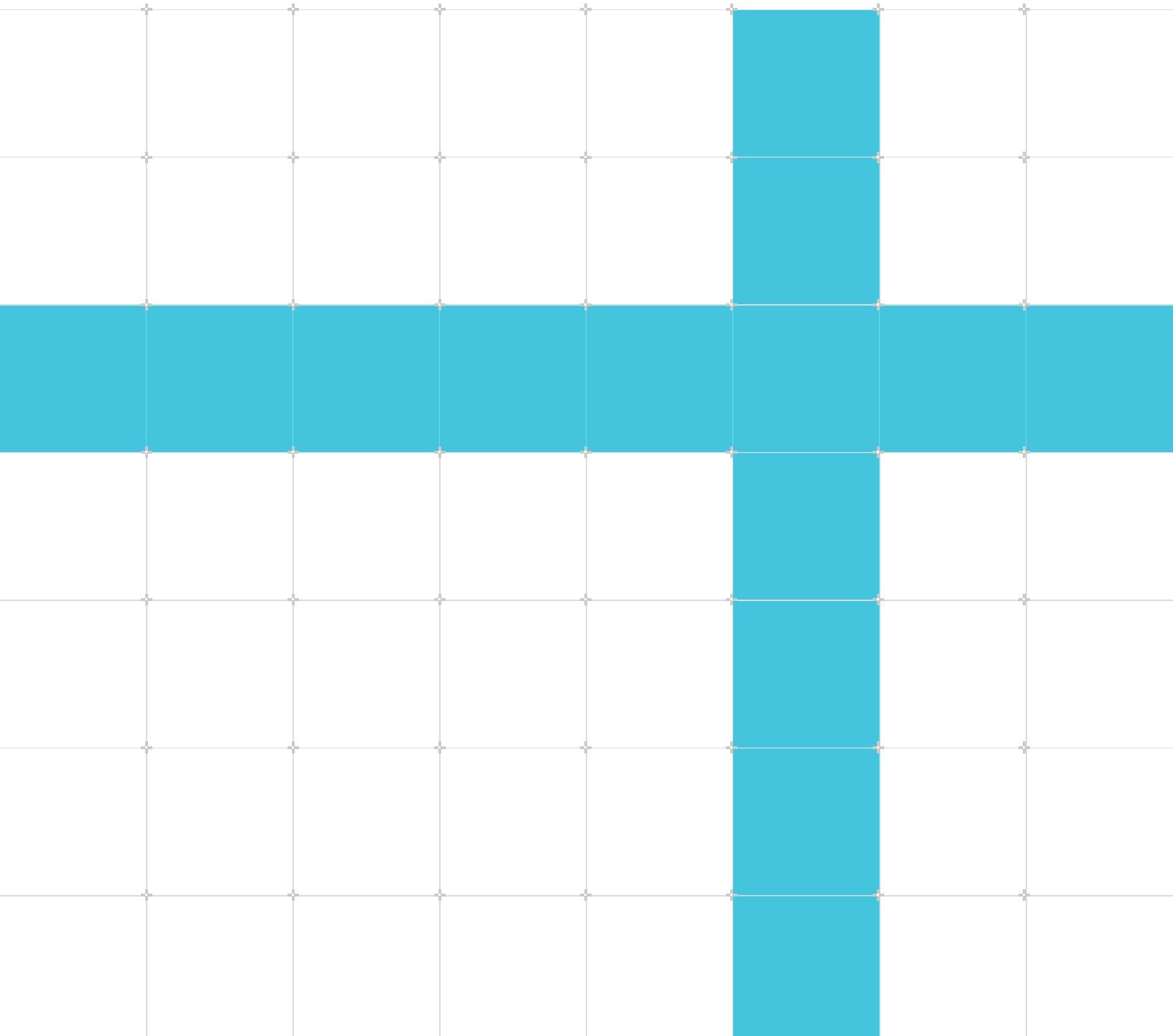
GPU-initiated Rowhammer attack

Version 1.0

Frequently Asked Questions

Issue 01
102853_0100_01_en



GPU-initiated Rowhammer attack

Frequently Asked Questions

Release information

Document history

Issue	Date	Confidentiality	Change
0100-01	3 May 2018	Non-Confidential	First release

Proprietary Notice

and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

(LES-PRE-20349)

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by Arm and the party that Arm delivered this document to.

Unrestricted Access is an Arm internal classification.

Product Status

The information in this document is Final, that is for a developed product.

Feedback

Arm® welcomes feedback on this product and its documentation. To provide feedback on the product, create a ticket on https://support.developer.arm.com

To provide feedback on the document, fill the following survey: https://developer.arm.com/documentation-feedback-survey.

Inclusive language commitment

Arm values inclusive communities. Arm recognizes that we and our industry have used language that can be offensive. Arm strives to lead the industry and create change.

We believe that this document contains no offensive language. To report offensive language in this document, email terms@arm.com.

Contents

1 Frequently Asked Questions

The following information provides answers to some frequently asked questions about GPU-initiated 'Rowhammer' attacks.

Can you explain the problem in layman's terms?

Security researchers have demonstrated a GPU-initiated microarchitectural attack via a WebGL program enabling them to construct pointers to arbitrary virtual memory locations.

The method is using side-channel and so-called 'Rowhammer' attacks from remote JavaScript.

The so-called 'Rowhammer' attack has existed for several years, but recent research has shown such an attack can potentially be initiated from a GPU.

What kind of data is vulnerable?

Malware using this method and running remotely via a WebGL program could expose sensitive data on the system.

What is a 'Rowhammer' attack?

The so-called 'Rowhammer' attack was initially found by researchers in 2014 and the Project Zero at Google revealed two working privilege escalation exploits in 2015.

It is a side effect of DRAM. By frequently activating specific rows an attacker can influence the charge in the capacitors of adjacent rows, making it possible to induce bit flips in a victim row without having access to its data.

What is WebGL and how can it be used for a so-called 'Rowhammer' attack?

WebGL (Web Graphics Library) is a JavaScript API for rendering interactive 3D and 2D graphics within any compatible web browser without the use of plug-ins. Malware can use it for remote so-called 'Rowhammer'-type attacks via GPU acceleration.

What does this mean for the average mobile user?

Such an attack could potentially allow for unauthorized access to sensitive data on mobile devices.

What did you do upon being notified?

We took the immediate action to assess the scope of impact and worked together as an industry-wide effort. We have communicated the mitigation measures to all affected silicon partners. There was no delay between Arm partners providing details of the new technique and Arm starting to take action.

What consumer products are affected?

GPUs are a common part of consumer products, such as mobile phones, DTVs, and VR devices. The most recent exploit described here utilizes the GPU to initiate a so-called 'Rowhammer' attack. There are software mitigations to address it.

What Mali GPUs are impacted?

It may be possible that variants of the exploit discovered by the researchers could be found on Mali GPUs.

We are not aware of any such exploits on Mali GPUs and believe that the memory structure and internal timing of Mali GPUs would make it difficult to implement.

Are Mali GPUs safer than others?

We have no comments on non-Mali GPUs. However, as previously stated, our assessment is that it will be difficult to find such an exploit on Mali GPUs.

Are software mitigations available, and will I get them?

Yes, there are software mitigations in web browsers to disable the high-resolution timer or to provide a less accurate timer. Google has disabled the high-resolution timer in Chrome. Please ensure your browser is up-to-date in line with good practice.