NEWS

RAMpage attack unlikely to pose real-world risk says expert

The RAMpage attack against the Rowhammer vulnerability in Android devices is theoretically possible, but may be more academic than it is a practical concern said one expert.


Michael Heller
Senior Reporter
03 Jul 2018
Follow

A group of researchers developed a proof of concept for a variant of the Rowhammer exploit against Android devices and proved that Google's protections aren't enough, but one expert said the RAMpage attack is unlikely to pose a real-world threat.

A team of researchers from Vrije Universiteit Amsterdam, the University of California at Santa Barbara, Amrita University of Coimbatore, India and EURECOM -- including many of the researchers behind the Drammer PoC attack upon which RAMpage was built -- and created both the RAMpage attack against ARM-based Android devices and a practical mitigation, called GuardION.

According to the researchers, the most likely method for attacking a Rowhammer vulnerability on a mobile device is through a direct memory access (DMA) based attack.

As such, they developed the RAMpage attack, "a set of DMA-based Rowhammer attacks against the latest Android OS, consisting of (1) a root exploit, and (2) a series of app-to-app exploit scenarios that bypass all defenses," researchers wrote in their research paper. "To mitigate Rowhammer exploitation on ARM, we propose GuardION, a lightweight defense that prevents DMA-based attacks -- the main attack vector on mobile devices -- by isolating DMA buffers with guard rows."

The researchers said a successful RAMpage attack could allow a malicious app to gain unauthorized access to the device and read secret data from other apps, potentially including "passwords stored in a password manager or browser, personal photos, emails, instant messages and even business-critical documents." However, lead researcher Victor van der Veen was careful to note it is unclear how many devices are at risk because of differences in software.

"With RAMpage, we show that the software defenses that were deployed to stop Drammer attacks are not sufficient. This means that the only remaining requirement is having buggy hardware. Since we have seen bit flips on devices with LPDDR2, LPDDR3, and LPDDR4 memory, we state that all these devices may be affected, although it is uncertain how many," van der Veen wrote via email. "Local access is required. This means that the attacker must find a way to run code (e.g., an app) on the victim's device. A second requirement is that the device needs to be vulnerable for the Rowhammer bug: it is unclear what percentage of devices expose this issue."

In a statement, Google downplayed the dangers of the RAMpage attack: "We have worked closely with the team from Vrije Universiteit and though this vulnerability isn't a practical concern for the overwhelming majority of users, we appreciate any effort to protect them and advance the field of security research. While we recognize the theoretical proof of concept from the researchers, we are not aware of any exploit against Android devices."

Google also asserted that newer devices include protections against Rowhammer attacks and "the researcher proof of concept for this issue does not work on any currently supported Google Android devices," though Google did not specify what qualified as a "currently supported Google Android device."

Liviu Arsene, senior e-threat researcher at Romania-based antimalware firm Bitdefender, said this could mean "that 'currently supported devices' refers to Android builds to which Google still issues security patches, which means that Android Marshmallow (6.0.) and above may not be susceptible" to the RAMpage attack. According to Google's latest platform numbers, more than 62% of Android devices in the wild are above this threshold.

However, van der Veen thought Google might be referring to its own handsets.

"I believe they hint at the devices that fall under their Android Reward program, which is basically the Pixel and Pixel 2. We did manage to flip bits on a Pixel, and I think that it is likely that there are Pixel phones out there on which the attack will work," van der Veen wrote. "I don't see criminals exploiting the Rowhammer bug in a large-scale fashion. It is more likely to be used in a targeted attack. I do think that Google can do a bit more though."

Arsene agreed that the RAMpage attack does appear "very difficult and unlikely to happen on a mass scale."

"Attackers would have to know in advance the type of device the target owns, because some manufacturers and OS builds implement different row sizes (e.g. 32KB, 64KB, 128KB), making the attack significantly more complex and less reliable," Arsene wrote via email. "Google may be right in saying the attack should not be of concern to average users, but it could be used in highly targeted attacks that involve stealthily compromising the device of a high priority individual. For mass exploitation of Android devices there are likely other, less sophisticated methods, for compromise. Attackers will often go for the path of least resistance that involves maximum efficiency and minimum effort to develop and deploy."

GuardION defense

Despite the relatively low likelihood of the RAMpage attack being used in the wild, researchers developed a mitigation based on protecting Google's ION DMA buffer management APIs, which were originally added to Android 4.0.

"The main reason for which defenses fail in practice is because they aim to protect all sensitive information by making sure that they are not affected by Rowhammer bit flips. Hence, they are either impractical or they miss cases," the researchers wrote in their paper. "Instead of trying to protect all physical memory, we focus on limiting the capabilities of an attacker's uncached allocations. This enforces a strict containment policy in which bit flips that are triggered by reading from uncached memory cannot occur outside the boundaries of that DMA buffer. In effect, this design defends against Rowhammer by eradicating the ability of the attacker to inject bit flips in sensitive data."

Van der Veen added via email, "I think they main message should be that Rowhammer-based exploits are still possible, despite Google's efforts. I think there is also (scientific) value in our breakdown of other proposed mitigation techniques and how they apply to mobile devices, plus our proposed defense, GuardION."

GuardION may not be real-world ready either though. The researchers noted that Google said the mitigation technique resulted in too much "performance overhead" in apps, but they continue to work with the Android security team "to figure out what a real-world benchmark looks like so that we can hopefully improve our implementation."

Arsene said "the existence of security research that exploits hardware vulnerabilities does not necessarily mean that users will be more at risk than before."

"Some of it is purely academic and the practical applications of weaponizing this type research may never become a reality for the masses," Arsene wrote. "However, users should realize that unpatched, outdated, and unsupported devices and operating systems will always involve significant security risks to their privacy and data."