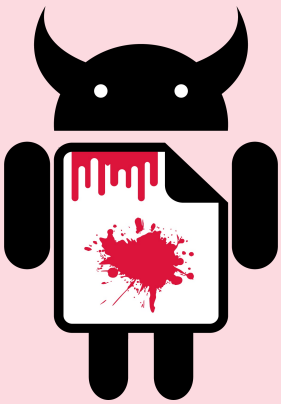
RAMPAGE AND GUARDION

Vulnerabilities in modern phones enable unauthorized access.

RAMPAGE exploits a critical vulnerability in modern phones that allows apps to gain unauthorized access to the device. While apps are typically not permitted to read data from other apps, a malicious program can craft a RAMPAGE exploit to get administrative control and get hold of secrets stored in the device. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

RAMPAGE works on Android devices, including smartphones and tablets. It is not unlikely that similar attacks are possible on Apple products or even regular personal computers and the cloud.

GUARDION is an award-winning prototype defense mechanism that stops RAMPAGE attacks.



RAMPAGE

RAMPAGE breaks the most fundamental isolation between user applications and the operating system. This attack allows an app to take full administrative control over the device.

If your device is shipped with vulnerable memory and runs with an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking it. Unfortunately, there are no software patches against RAMPAGE deployed yet.

GUARDION

GUARDION defends against RAMPAGE attacks. It prevents an attacker from modifying critical data structures by carefully enforcing a novel isolation policy. GUARDION won the best research award at the International Conference on Computing Systems (CompSys 2018).

Although GUARDION is not deployed in operating systems yet, there are ongoing efforts to realize this. The source code for GUARDION is available online in the form of an Android kernel patch.

RAMPAGE paper | cite

GUARDION source | cite

The team behind RAMPAGE and GUARDION

RAMPAGE and GUARDION are the result of an international collaboration of system security researchers:

- **Victor van der Veen**, MSc.
  Vrije Universiteit Amsterdam
- Dr. **Martina Lindorfer**
  TU Wien
- Dr. **Yanick Fratantonio**
  EURECOM
- Harikrishnan Padmanabha Pillai, MSc.
  IBM
- Prof. Dr. **Giovanni Vigna**
  UC Santa Barbara
- Prof. Dr. **Christopher Kruegel**
  UC Santa Barbara
- Prof. Dr. **Herbert Bos**
  Vrije Universiteit Amsterdam
- Dr. **Kaveh Razavi**
  Vrije Universiteit Amsterdam

CONTRIBUTE TO RESEARCH

We developed an Android app to test whether your device might be vulnerable to RAMPAGE attacks. The core of our app consists of a component for which we also released the **source code**. After a successful run, the app uploads anonymized output. We will use this to get a better understanding of how many devices are vulnerable. Of course, you can opt out of sharing results.

Download it.

Questions & Answers

Am I affected by the vulnerability?

That is unclear. You can get some level of indication by running our **test app**.

Can I detect if someone has exploited RAMPAGE against me?

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

Can my antivirus app detect or block this attack?

While possible in theory, this is unlikely in practice. Unlike usual malware, RAMPAGE is 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 take full control over your device and access anything on it. This may include passwords and sensitive data stored on the system.

Has RAMPAGE been abused in the wild?

We don't know.

Is there a workaround/fix?

No. The only efforts that we are aware of is our own work, GUARDION.

What systems are affected by RAMPAGE?

Android-based devices may be affected by RAMPAGE. More technically, every mobile device that is shipped with LPDDR2, LPDDR3, or LPDDR4 memory is potentially affected, which is effectively every mobile phone since 2012. We successfully tested RAMPAGE on an LG G4. At the moment, it is unclear whether desktop operating systems are also affected, but this seems very likely.

What is the difference between RAMPAGE and GUARDION?

GUARDION is a defense to mitigate RAMPAGE attacks.

Why is it called RAMPAGE?

The vulnerability basically rams memory pages to obtain arbitrary read and write access.

Why is it called GUARDION?

The name is based on the Android memory subsystem called ION that RAMPAGE uses. By inserting guards, RAMPAGE attacks become much harder.

What is GUARDIONS OF THE GALAXY?

That would be our GUARDION defense deployed on any Samsung model.

Is there more technical information about RAMPAGE and GUARDION?

Yes, there is an **academic paper** about RAMPAGE and GUARDION.

What is CVE-2018-9442?

CVE-2018-9442 is the official reference to RAMPAGE. CVE is the Standard for Information Security Vulnerability Names maintained by MITRE.

Can I see RAMPAGE in action?

No.

Can I use the logo?

Yes. And please get us a T-shirt while you're at it. And stickers. We like stickers.

Is there a proof-of-concept code?

No, not for the RAMPAGE attack. Our implementation of the GUARDION defense, however, is open source and available at **github.com/vusec/guardion**.

Why does this page look like the Spectre and Meltdown websites?

You mean like **this**? Because imitation is the sincerest form of flattery. This page is obviously a nod towards the huge (and in our eyes truly deserved) Spectre/Meltdown hype from earlier this year. **It should be clear that RAMPAGE is not even close to being the next Spectre.** Having said that, we (1) like our logos, and (2) hope that this page gets more people involved in **contributing to research**: It is currently unclear how widespread the Rowhammer bug (the hardware error that RAMPAGE exploits) is. By getting more people to run our updated DRAMMER test app, we hope to get a better understanding of this issue, allowing us to make decisions on how to move forward (i.e., should we continue looking for defenses or is this an already-solved problem?)

What does Google think of this?

Google acknowledges the issue (hence CVE-2018-9442). Unfortunately, they concluded that GUARDION results in more "performance overhead" on real-world apps than we report in our paper. We are in communication with the Android security team to figure out what a real-world benchmark looks like so that we can hopefully improve our implementation.

We received the following statement from Google:
We have worked closely with the research team 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 also recognize that newer devices contain memory with Rowhammer specific protections (for example the researcher proof of concept for this issue does not work on any currently supported Google Android devices).