SIGN UP HERE

Security

Oh, great, now there's a SECOND remote Rowhammer exploit

Send enough crafted packets to a NIC to put nasties into RAM, then the fun really starts

By Richard Chirgwin 17 May 2018 at 01:35 18 SHARE ▼

Hard on the heels of the first network-based Rowhammer attack, some of the boffins involved in discovering Meltdown/Spectre have shown off their own technique for flipping bits using network requests.

With a gigabit connection to the victim, the researchers reckon, they can induce security-critical bit flips using crafted quality-of-service packets.

Advertisement

SIGN UP HERE

Last week, we reported on research called “Throwhammer” that exploited Rowhammer via remote direct memory access (RDMA) channels.

In separate research, Meltdown/Spectre veterans Daniel Gruss, Moritz Lipp and Michael Schwarz of Graz University of Technology and their team have published a paper describing Nethammer (their co-authors are Lukas Lamster and Lukas Raab, also of Graz; Misiker Tadesse Aga of the University of Michigan; and Clémentine Maurice of IRISA at the University of Rennes).

Nethammer works, they said, without any attacker-controlled code on the target, attacking “systems that use uncached memory or flush instructions while handling network requests.

> **“Depending on the location, the bit flip compromises either the security and integrity of the system and the data of its users, or it can leave persistent damage on the system, ie, persistent denial of service”.**

Here's a quick recap of Rowhammer to help understand how Nethammer works: by rapidly writing and rewriting memory, it induces capacitor errors in DRAM, and the resulting data corruption can be manipulated to gain control over the victim's machine.

In its original form, Rowhammer let an attacker escalate their privilege to kernel level, but you needed access to the victim machine.

Nethammer mounts remote attacks by exploiting the memory used for packet processing, if you can send enough of them.

'Rowhammer' attack flips bits in memory to root Linux

READ MORE →

“Nethammer sends a crafted stream of network packets to the target device to mount a one-location or single-sided Rowhammer attack by exploiting quality-of-service technologies deployed on the device,” the paper explains.

“For each packet received on the target device, a set of addresses is accessed, either in the kernel driver or a user-space application processing the contents.”

In normal circumstances, caching would make an attack difficult, so the Graz team worked out how to bypass the cache and send their attacks “directly into the DRAM to cause the row conflicts required for hammering”.

If the victim's machine is susceptible to single-sided hammering and has DDR2, DDR3 or DDR4 memory installed, the group demonstrated working attacks on personal computers and on virtual machines running in cloud environments.

Advertisement

SIGN UP HERE

The good news? The best mitigation is to have systems that defend network connections against traffic spikes, because an attacker needs to fire a lot of packets at the target: “In our experiments, we sent a stream of UDP packets with up to 500 Mbps to the target system. We were able to induce a bit flip every 350 ms”, the paper notes.

Brief spikes at high throughput could get past such defenses, however. ®

Sponsored: Continuous Lifecycle London 2018 - Early Bird Tickets Now Available

Tips and corrections

18 Comments

Sign up to our Newsletter
Get IT in your inbox daily

More from The Register

Rowhammer RAM attack adapted to hit flash storage
Project Zero's two-year-old dog learns a new trick

RAM, bam, awww ... man! Boffins defeat Rowhammer protections
New attack flips bits in uerspace binaries for fun and p0wnage

Rowhammer strikes networks, Bolton strikes security jobs, and Nigel Thornberry strikes Chrome, and more
ROUNDUP Hacking laws in the limelight in Georgia and DC, plus new iPhone anti-tampering

App proves Rowhammer can be exploited to root Android phones – and there's little Google can do to fully kill it
Hardware vuln strikes 18 of 27 tested mobes

Google's PHP API client has XSS vulnerability
Patch promised

Patch or ditch Adobe Flash: Exploit on sale, booby-trapped Office docs spotted in the wild
ThreadKit leverages flaw fixed in February

Whitepapers

Reshaping ECM: new opportunities in the cloud

Forward-looking CIOs understand that content management is a moving target.

Remedying the Email Security Gaps in Microsoft Office 365

If you have made the move to Microsoft Office 365™ or imminently plan to, you are in good company.

Data Architecture for IoT Communications and Analytics

This checklist explores some fundamental aspects of the data architecture necessary for IoT success.

5 crucial questions to ask your cloud service provider

Breaking up can be hard to do – just ask the UK and the European Union.

Sponsored links

Get The Register's Headlines in your inbox daily - quick signup!

About us›

- Who we are
- Under the hood
- Contact us
- Advertise with us

More content›

- Week’s headlines
- Top 20 stories
- Alerts
- Whitepapers

Situation Publishing›

- The Next Platform
- Continuous Lifecycle London
- M-cubed
- Webinars

SITUATION PUBLISHING

The Register - Independent news and views for the tech community. Part of Situation Publishing

Sign up to our Newsletters

Join our daily or weekly newsletters, subscribe to a specific section or set News alerts

Subscribe ›

Biting the hand that feeds IT © 1998–2018