Pwnie Award Winners 2023

Best Desktop Bug
@b2ahex
CountExposure! (Local PrivilegeEscalation in Windows PerformanceCounters): CVE-2022-22036

Best Cryptographic Attack
Ben Nassi
Video-based Cryptanalysis: Extracting Cryptographic Keys from Video Footage of a Device’s Power LED: https://eprint.iacr.org/2023/923

Best Song
Ohm-I
Clickin' by Ohm-I (https://mcohmi.bandcamp.com/track/clickin)

Most Innovative Research
@ghidraninja
INSIDE APPLE’S LIGHTNING: JTAGGING THE IPHONE FOR FUZZING AND PROFIT (https://www.youtube.com/watch?v=8p3Oi4DL0eI&t=1s)

Most Under-hyped Research
Simon Zuckerbraun at Trendmicro
Activation Context Cache Poisoning: A new class of Window LPE bugs (https://www.thezdi.com/blog/2023/1/23/activation-context-cache-poisoning-exploiting-csrss-for-privilege-escalation)

Best Privilege Escalation
@danis_jiang and @0x140ce
URB Excalibur: Slicing Through the Gordian Knot of VMware VM Escapes (CVE-2022-31705, https://www.vmware.com/security/advisories/VMSA-2022-0033.html)

Best RCE Bug
@scannell_simon
ClamAV RCE (CVE-2023-20032): ASLR bypass technique enabling 0 click server side exploits

Lamest Vendor Response
Threema
Three Lessons From Threema: Analysis of a Secure Messenger (A new canonical example for "blog post of butthurt": https://threema.ch/en/blog/posts/news-alleged-weaknesses-statement)

Most Epic Fail
The Transportation Security Administration
TSA Leaving the entire no fly list exposed on a server

Most Epic Achievement
Clement Lecigne
0-days hunter world champion: Clement Lecigne burning dozens of 0-days in the wild