Pwnie for Best Crypto Bug

X.509DoS	Exploiting and Detecting Denial-of-Service Vulnerabilities in Cryptographic Libraries using Crafted X.509 Certificates	Bing Shi, Wenchao Li, Yuchen Wang, Xiaolong Bai, and Luyi Xing
Untangling the Knot	Breaking Access Control in Home Wireless Mesh Networks	Xinan Zhou
EntrySign	“It turned out that AMD had been using the example key from the NIST specification for over 7 years.”	Matteo Rizzo, Kristoffer Janke, Josh Eads, Tavis Ormandy, Eduardo Vela Nava

Pwnie for Best Desktop Bug

EntrySign (Again)	“It turned out that AMD had been using the example key from the NIST specification for over 7 years.”	Matteo Rizzo, Kristoffer Janke, Josh Eads, Tavis Ormandy, Eduardo Vela Nava
BitUnlocker	Leveraging Windows Recovery to Extract BitLocker Secrets	Alon Leviev (@alon_leviev) Netanel Ben Simon (@NetanelBenSimon)

Pwnie for Best Mobile Bug

Profile Pin Bypass - Jio Hotstar	A simple bug no one thought existed in JioHotstar which allowed them to bypass Profile Pins of locked account users on the same or different accounts.	@Ravenzbb
Exploiting the Samsung Galaxy S24 at Pwn2Own	During Pwn2Own Ireland, Ken Gannon of NCC Group used multiple bugs to get a shell and install an app on the Samsung Galaxy S24. At a high level, the chain consists of: - Bugs 1 and 2 – Use a Browsable Intent to launch Gaming Hub and open a WebView to a custom URL with JavaScript enabled - Bug 3 – Force Gaming Hub to start arbitrary exported Activities - Bug 4 – Force the phone to download arbitrary files from a nearby phone - Bug 5 – A file downloaded via Quick Share can be saved to an arbitrary location - Bugs 6 and 7 – Silently install .apk file located on disk When these bugs are combined, they result in rogue applications being installed on the device. The chain won him $50,000 at the Pwn2Own contest.	Ken Gannon of NCC Group

Pwnie for Best Song (Nothing - Thank God)

Pwnie for Best Priv Esc

Linux Kernel VSOCK Quadruple Race Condition	This vuln is an extreme race condition in the Linux kernel's VSOCK, where precisely orchestrating a race among four threads can trigger a Use-After-Free.	https://x.com/v4bel https://x.com/_qwerty_po
BadSuccessor	"BadSuccessor" a vulnerability uncovered by Yuval Gordon of Akamai in Microsoft's implementation of dMSA that could enable low-privileged users to compromise any user in Active Directory	https://x.com/YuG0rd
Microsoft Windows MSI Installer - Repair to SYSTEM	The MSI installer research (CVE-2024-38014) resulted in multiple local privilege escalation advisories for different products. Instead of pursuing thousands of affected products, we went straight to the source for a fix: Microsoft.	Michael Baer

Pwnie for Best RCE

CVE-2024-38077 (MadLicense)	CVE-2024-38077, which impacts all versions of Windows Server from 2003 to 2025. Despite Microsoft's various fortifications to Windows for decades and we didn't see preauth 0-click RCE in Windows for years, they still can exploit a single memory corruption vulnerability to complete the 0-click preauth RCE on Windows. They can bypassing all the mitigations on the latest Windows Server 2025 and build a 0-click preauth RCE exploit by using only CVE-2024-38077.	Zhiniang Peng - Associate Professor, Huazhong University of Science and Technology Ver - Security Researcher Zishan Lin - Security Researcher
Samsung Mobile Video Call 1-click RCE	Remote, One-Click: Breaking into Smartphones via a Non-Well-Known Remote Attack Surface @ BH 2024	@2st___ @Fantasyoung_ @Thankkong

regreSSHion (CVE-2024-6387)	A pre-authentication RCE in OpenSSH's server, default configuration; the first one in nearly 20 years! An unusual vulnerability, too: a signal handler race condition that leads to an exploitable heap corruption.	https://x.com/qualys (They .txt formatted their submission i love these guys)

Pwnie for Epic Achievement

Not one but two vulnerabilities in OpenSSH!	Two vulnerabilities in OpenSSH, one of the most secure software in the world: CVE-2024-6387 (regreSSHion), an exploitable pre-authentication RCE in OpenSSH's server, default configuration (the first one in ~20 years!); and CVE-2025-26465, a machine-in-the-middle attack against OpenSSH's client (FreeBSD was vulnerable to this by default for ~10 years!).	Qualys!
Prompt Injection as a Defense Against LLM-driven Cyberattacks	This paper turns the tables on AI-driven attackers by weaponizing LLM vulnerabilities for defense. Mantis, the proposed system, uses prompt injection not as a risk but as a countermeasure, luring LLM agents into sabotaging themselves or falling into inescapable tarpit traps. Demonstrating over 95% success against real-world LLM agents, it is the first to show how large language models can be hacked back through their own automation pipelines. This work doesn't just defend against LLM-powered attacks—it convinces the attackers' own AI to pull the trigger on itself.	Pasquini, Kornaropoulos, Ateniese
MIFARE Classic: exposing the static encrypted nonce variant... and a few hardware backdoors	For years The FM11RF08(S) variants of MIFARE Classic were considered unbreakable in practice based on previously published methods. Philippe Teuwen found ways to break these cards without requiring any prior knowledge of card keys, a feat previously thought to be impossible for this variant. He also found a hardware backdoor in these cards.	Philippe Teuwen aka doegox

Pwnie for Epic Fail

SignalGate - Novel Signal Bypass	Is it still leaking material if you just add them to the group chat?	Mike Waltz
The creepy Stalkerware industry and its never-ending data breaches	According to TechCrunch's tally, counting the latest data exposure of Catwatchful, there have been at least 26 stalkerware companies since 2017 that are known to have been hacked, or leaked customer and victims' data online.	Any representatives of the stalkerware industry that would like to claim credit. Or Tal Dilian.

Pwnie for Lamest Vendor Response

Linux CVE CNA - Again CVE-2025-0927 - Linux kernel slab OOB write in hfsplus	They're still tripping over themselves - it's a whole thing. Idk man nobody is getting paid for this shit and everything runs on it.	Linus fix pl0x
Profile Pin Bypass	Simply denied it all. Marked the bugs as - informative, internally known, n/a without proper explanation.	Jio Hotstar
Typical nonsense	Someone ignored a report etc / didn't mark a bounty / etc etc	Buncha people

Pwnie for Most Innovative

BitUnlocker: Leveraging Windows Recovery to Extract BitLocker Secrets	This work explores a novel attack vector targeting the Windows Recovery Environment (WinRE) to attack and bypass BitLocker.	Alon Leviev (@alon_leviev) Netanel Ben Simon (@NetanelBenSimon)
Invitation is All You Need! Invoking Gemini for Workspace Agents with a Simple Google Calendar Invite	The researchers (Ben Nassi Stav Cohen and Or Yair) showed that by inviting a victim to a Google Calendar meeting whose subject contains an indirect prompt injection, attackers could hijack the application context and invoke its integrated agents, and exploit their permission to perform malicious activities.	@ben_nassi
Haunted by Legacy: Discovering and Exploiting Vulnerable Tunnelling Hosts	Researchers discovered that more than 4 million servers on the internet accept old unauthenticated	Angelos Beitis

	tunneling traffic such as IPIP, GRE, 6in4, 4in6, and so on. This enabled them to trivially spoof source IP addresses, perform denial-of-service attacks, and even access the private network of companies.	

Pwnie for Most Underhyped Research

KernelSnitch	KernelSnitch is a software-induced side-channel attack targeting the Linux kernel. It is the first known side-channel technique capable of leaking kernel heap pointers without relying on potentially unstable memory-corruption vulnerabilities.	Lukas Maar
Scheduled Disclosure	Scheduled Disclosure shows that the power management algorithms of modern Intel processors enable turning power side-channel attacks into remote timing attacks in a way that is more effective than previously demonstrated and works even in the absence of frequency side-channel leakage.	Inwhan Chun Isabella Siu Riccardo Paccagnella
How hard can it get? Hardy Barth charging station mess	Hardy Barth EV charging station products are affected by critical vulnerabilities that can be exploited through both physical access and unauthenticated network access. These vulnerabilities pose significant risks, including system compromise, data breaches, and operational disruptions within EV charging infrastructures. But the vendor was "occupied" with other tasks than security and later did not provide any timeline for a fix.	Stefan Viehböck