The Good Faith Cybersecurity Researchers Coalition

Community Newsletter, December 2023

GFCRC Updates

Zoltán Balázs Interview

Head of Vulnerability Research at CUJO AI Zoltán Balázs shares his insights and experiences around challenges surrounding vulnerability research and bug fixes in IoT systems - networked security cameras, DVRs, and other appliances - around the world.

https://youtu.be/CM3ij8VKyQY

GFCRC Substack Online

The GFCRC now has a substack for updates, blog posts, and announcements: https://gfcrc.substack.com/

Industry, Regulatory, Technology News

Swiss Federal Council Issues Recommendations on Ethical Hacking, CVD

The Swiss federal council adopted a set of recommendations on ethical hacking, including institutionalizing both responsible vulnerability research and coordinated vulnerability disclosure, creating clearer rules that permit ethical hacking under defined circumstances, and improving cooperation with industry.

NCSC-CH announcement, EFD publication (DE)

PDF (German) text of the announcement

EU Cyber Resilience Act (CRA) Reaches Political Agreement

The European Commissioned cleared a major hurdle in the passage of the proposed Cyber Resilience Act, which puts significant responsibility on software and hardware makers, importers, and distributors. ICT products will fall under significant security and risk management requirements throughout their lifecycle.

EU announcement

CyAN analysis of the CRA

CISPA Paper: "Where Are the Red Lines? Towards Ethical Server-Side Scans in Security and Privacy Research"

CyAN member and CISPA researcher Florian Hantke and his team recently published a paper discussing perspectives, challenges, and restrictions around server-side vulnerability scanning, a major component of ethical cybersecurity vulnerability research.

Direct link (pdf)

Hackers Abusing GitHub to Evade Detection and Control Compromised Hosts (via The Hacker News)

"Threat actors are increasingly making use of GitHub for malicious purposes through novel methods, including abusing secret Gists and issuing malicious commands via git commit messages." The use of compromised

Original story