February 2, 2022

Intel Launches Project Circuit Breaker

A new expansion of its Bug Bounty program, Intel's Project Circuit Breaker brings together a community of elite hackers to reshape vulnerability management.

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **What's New:** Intel is expanding its Bug Bounty program with Project Circuit Breaker, bringing together a community of elite hackers to hunt bugs in firmware, hypervisors, GPUs, chipsets and more. Project Circuit Breaker broadens and deepens Intel's existing open Bug Bounty program by hosting targeted time-boxed events on specific new platforms and technologies, providing training and creating opportunities for more hands-on collaboration with Intel engineers. Project Circuit Breaker's first event, Camping with Tigers, is already underway with a group of 20 researchers who received systems with Intel® Core™ i7 processors (formerly "Tiger Lake").

> *"Project Circuit Breaker is possible thanks to our cutting-edge research community. This program is part of our effort to meet security researchers where they are and create more meaningful engagement. We invest in and host bug bounty programs because they attract new perspectives on how to challenge emerging security threats – and Project Circuit Breaker is the next step in collaborating with researchers to strengthen the industry's security assurance practices, especially when it comes to hardware. We look forward to seeing how the program will evolve and to introducing new voices to the meaningful work that we do."*
> –Katie Noble, director, Intel Product Security Incident Response Team (PSIRT) and Bug Bounty

How It Works: Through Project Circuit Breaker, Intel is creating a community dedicated to offering training to security researchers, exciting new hacking challenges and opportunities to explore at unprecedented levels with new and pre-release products, as well as new collaborations with Intel hardware and software engineers. Camping with Tigers launched in December and will end in May, with bounty multipliers being offered at three milestones for eligible vulnerabilities.

"Bug bounty programs are a powerful tool to continuously improve the security of our products," said Tom Garrison, vice president and general manager of Client Security Strategy & Initiatives at Intel. "Camping with Tigers – our first event under Project Circuit Breaker – brings together world-class security researchers and our own product engineers to deepen testing and improve resiliency on our 11th Gen Intel® Core™ processors. As we aim to develop the most comprehensive security features, we also realize the incredible value of deeper collaborations with the community to identify potential vulnerabilities and mitigate them for the ongoing improvement of our products."

Project Circuit Breaker will supplement Intel's existing open Bug Bounty program, which rewards researchers for original vulnerability findings on any eligible branded products and technologies. This program helps Intel to identify, mitigate and disclose vulnerabilities; in

2021, 97 of 113 externally found vulnerabilities were reported through Intel's Bug Bounty program. As demonstrated by Intel's Security-First Pledge, the company invests extensively in vulnerability management and offensive security research for the continuous improvement of its products.

Why It Matters: With Project Circuit Breaker, Intel is creating a more diverse and unified security community that is better prepared to address the industry's largest security concerns. New challenges, training, and unprecedented access to early products and Intel engineers will focus the talents of the community toward areas of high impact.

Since making the Bug Bounty program public in 2018, Intel has been advancing its investments in security by growing its team of security experts and increasing the company's emphasis on industry collaboration. Intel's security experts actively contribute to both the Bug Bounty Community of Interest, a forum for vendors, bug bounty managers and security researchers to exchange expertise and best practices, and FIRST (Forum of Incident Response and Security Teams). Enhancing vulnerability discovery and management internally, Intel adopted the secure development lifecycle (SDL) for both hardware and software. SDL has played a major role in helping to build a culture with a security-first mindset, where engineering teams drive more rigor and hold more accountability for security throughout the product lifecycle. Intel's Platform Update has also been refined to deliver predictable and bundled security updates to the community.

In addition to the Bug Bounty program, Intel Labs continues to cultivate leading-edge security research with the academic community. Some of this research has been recognized by the Intel Hardware Security Academic Award program, which awards top innovators for novel research with meaningful impact to the industry.

These efforts are driven by Intel's commitment to work in the open, be transparent and demystify the experience for security researchers. As new threats emerge and vulnerabilities are found, Intel remains committed to growing, adapting and relentlessly advancing security assurance through bug bounty programs, coordinated vulnerability disclosures and impactful researcher collaboration.

More Context: Project Circuit Breaker | Announcing Project Circuit Breaker | Intel's Bug Bounty Program | Product Security at Intel | Intel Hardware Security Academic Award

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

© Intel Corporation. Intel, the Intel logo and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20220202005276/en/

Jennifer Foss
1-425-765-3485
jennifer.foss@intel.com

Source: Intel Corporation