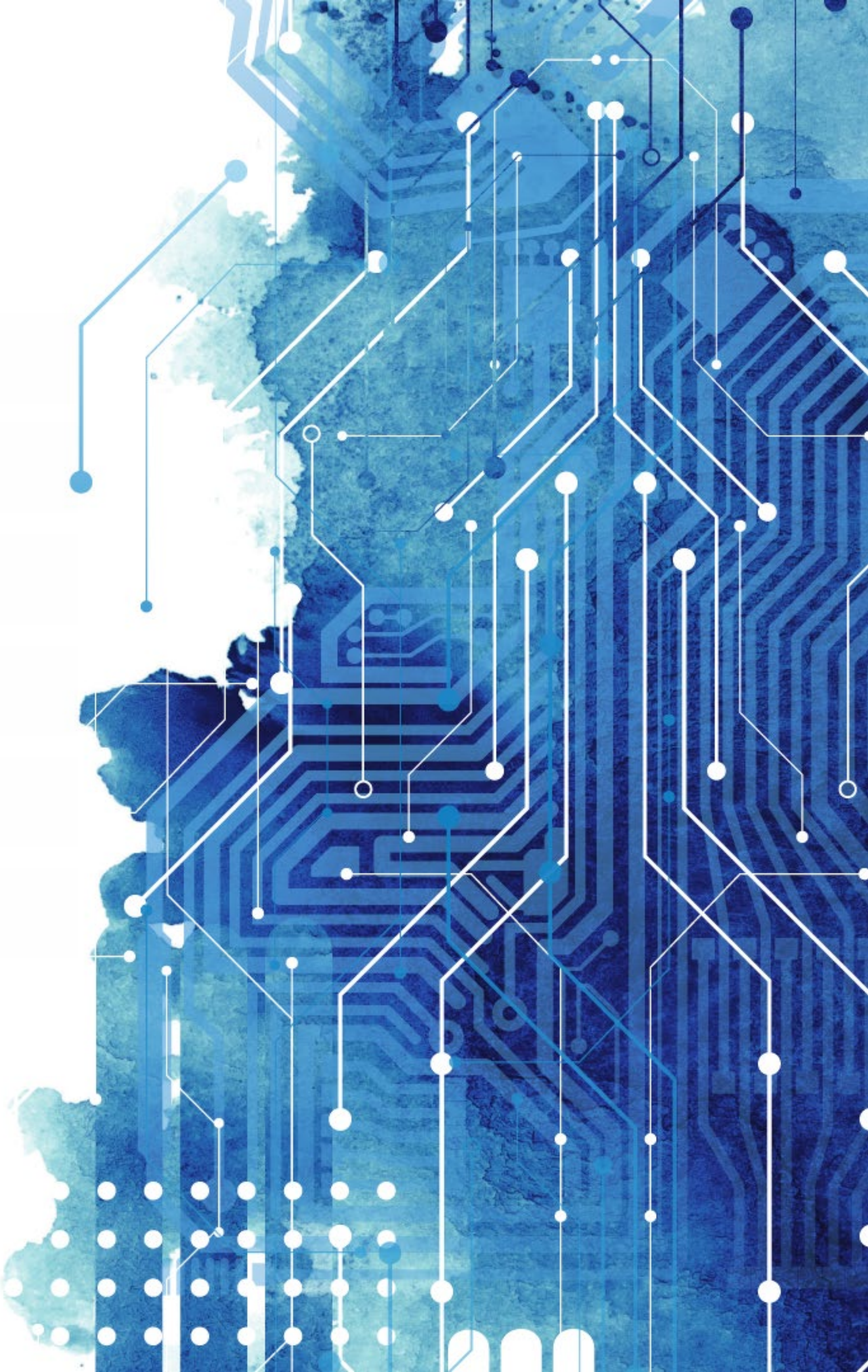
2023 Product Security Report

intel security

Table of Contents



Introduction

Security Starts with Intel

It is a given that any code with enough complexity will have bugs and potential vulnerabilities. A security-first commitment and an investment in product security assurance equal to the size and scope of a company's product market is essential as its customers rely on their ability to respond when an issue is discovered.

They should actively drive a security-first mindset across their organizations and invest heavily in discovering issues before a product ships. The very best are actively engaged across the industry in standards bodies and government affairs, funding academic research, and incentivizing and providing training to the security research community.

In a September 2023 blog post, Intel CEO Pat Gelsinger challenged readers to:

- Find a silicon vendor who takes as many steps and invests as much as we do to deliver more secure and resilient products to developers and customers.
- To all in the industry – evolve your product assurance practices, incident response, and mitigation to better protect customers' data and privacy.

He stated, "I'm so confident in how we look for potential vulnerabilities and the critical response to any identified that I would put the power of our product security assurance up against our direct competitors."

This report demonstrates the impact of Intel's active investments in product security assurance. We feel Intel's program is second to none in the silicon industry. For comparison, we will analyze publicly available data from Advanced Micro Devices, Inc. (AMD) to demonstrate the visible differences in assurance capabilities. More specifically, we look at the firmware that customers rely on to safeguard their data and privacy and believe that readers will see why Pat has such high confidence in Intel's capabilities.

Intel product security assurance leads the silicon industry
according to a recent study by ABI Research.

Intel's proactive product security assurance efforts account for
94% of vulnerabilities
disclosed in 2023.

In 2023, Intel's closest competitor had
3x more
platform firmware vulnerabilities than Intel.

Intel achieved a
39% reduction
in combined hardware and firmware vulnerabilities in 2023 compared to 2022.

Product Security Assurance

Product security assurance at Intel is an investment in people, processes, and tools extending from initial product development to the end of the product lifecycle. It means that customers can feel confident in Intel's Security-First Pledge and that we actively work to deliver security without sacrificing performance. By working with our customers and industry partners, we can achieve the levels of secure performance people expect and deliver the technology they trust.

Visit the following resources to learn more about Intel's approach to product security assurance:

Security-First Mindset

Learn how Intel works to shift our culture to a security-first mindset to fulfill our vision of empowering our customers with the most secure systems, software, and services driven by innovation to enhance the security capabilities they trust.

Secure Product Development

Learn more about Intel's security-first commitment, from an offensive security research team spanning ten countries to a robust Security Development Lifecycle (SDL) program baked into our product development.

Ongoing Product Security Assurance

Learn how Intel's security-first commitment does not end when a product ships. Discover how Intel's Product Security Incident Response Team (PSIRT) performs company-wide vulnerability management, how our innovative Bug Bounty Programs provide training and incentives to security researchers, and how our Intel Platform Update process enables an entire ecosystem to provide security updates to end customers.

How Intel Engages the Ecosystem

Learn more about how Intel engages the global ecosystem through deep engagement with the academic community, having a bias for open-source software, helping to drive security standards across the industry, and far-reaching community and policy advocacy.

Product Security Assurance: Competitive Assessment

A recent independent study by ABI Research* offers a comparative assessment and ranking of the Security Assurance Practices of the top silicon vendors. Findings:

Intel leads the silicon industry in product security assurance

Security Assurance Practices

Company	Score	Overall Ranking
Intel	82.2	1
Qualcomm	68.5	2
AMD	65.0	3
Nvidia	61.7	4
ARM	45.3	5

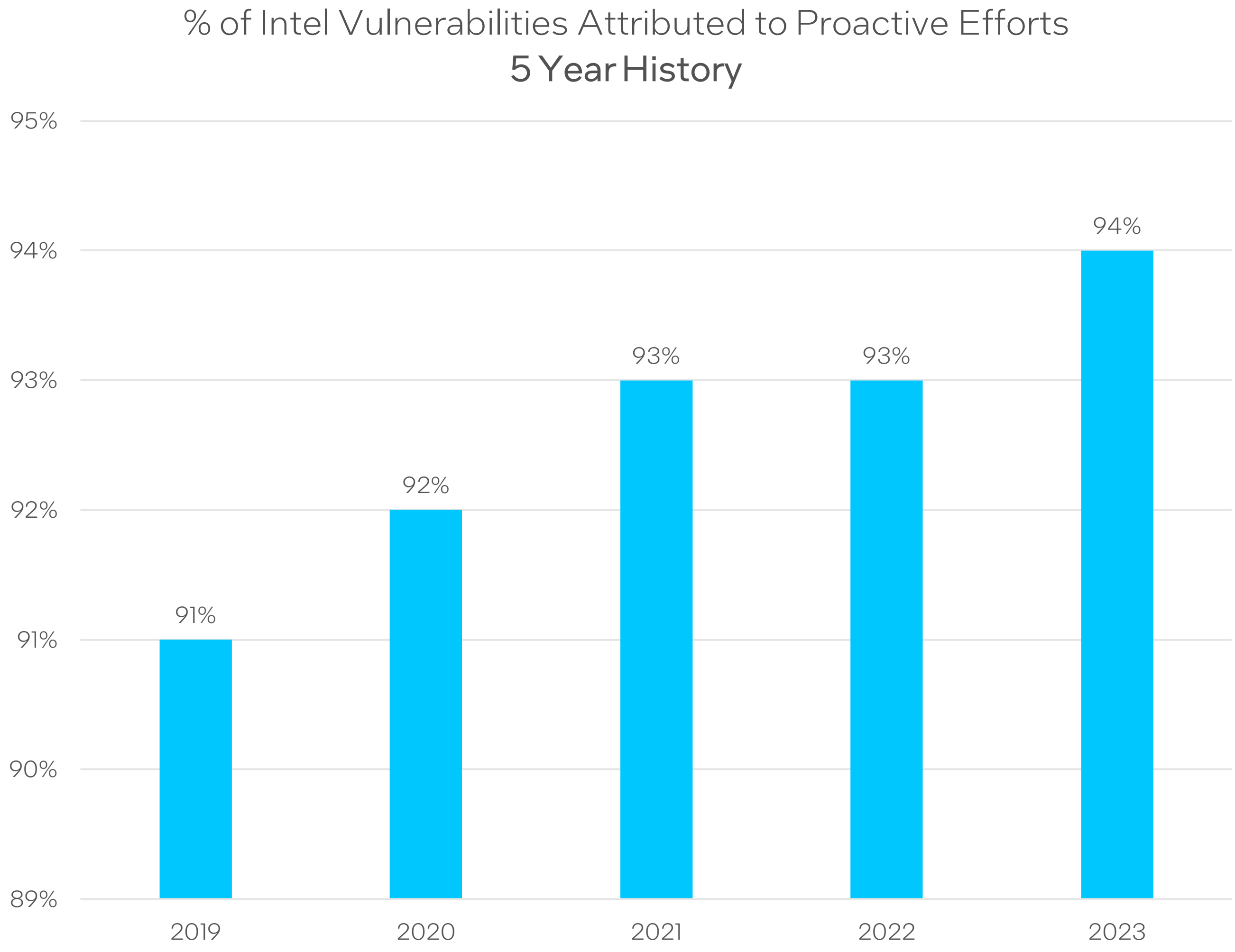
* Commissioned by Intel. Read the full report HERE

Summary of Intel 2023 Vulnerabilities

Proactive Product Security Assurance

Proactive product security assurance includes efforts to find vulnerabilities internally and through incentives to the external security research community via Bug Bounty Programs.

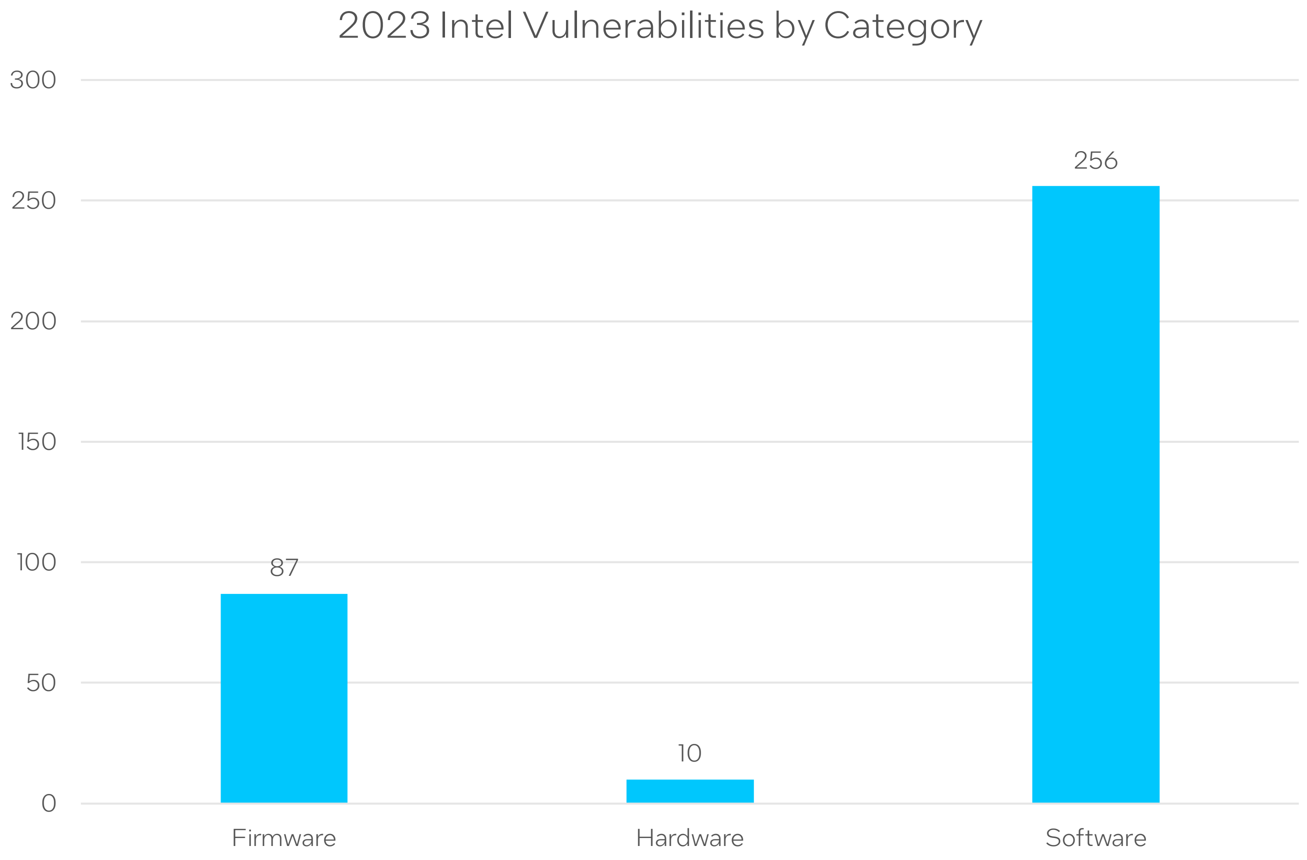
In 2023, Intel's proactive product security assurance investments accounted for 94% of the publicly disclosed vulnerabilities.



Summary of Intel 2023 Vulnerabilities

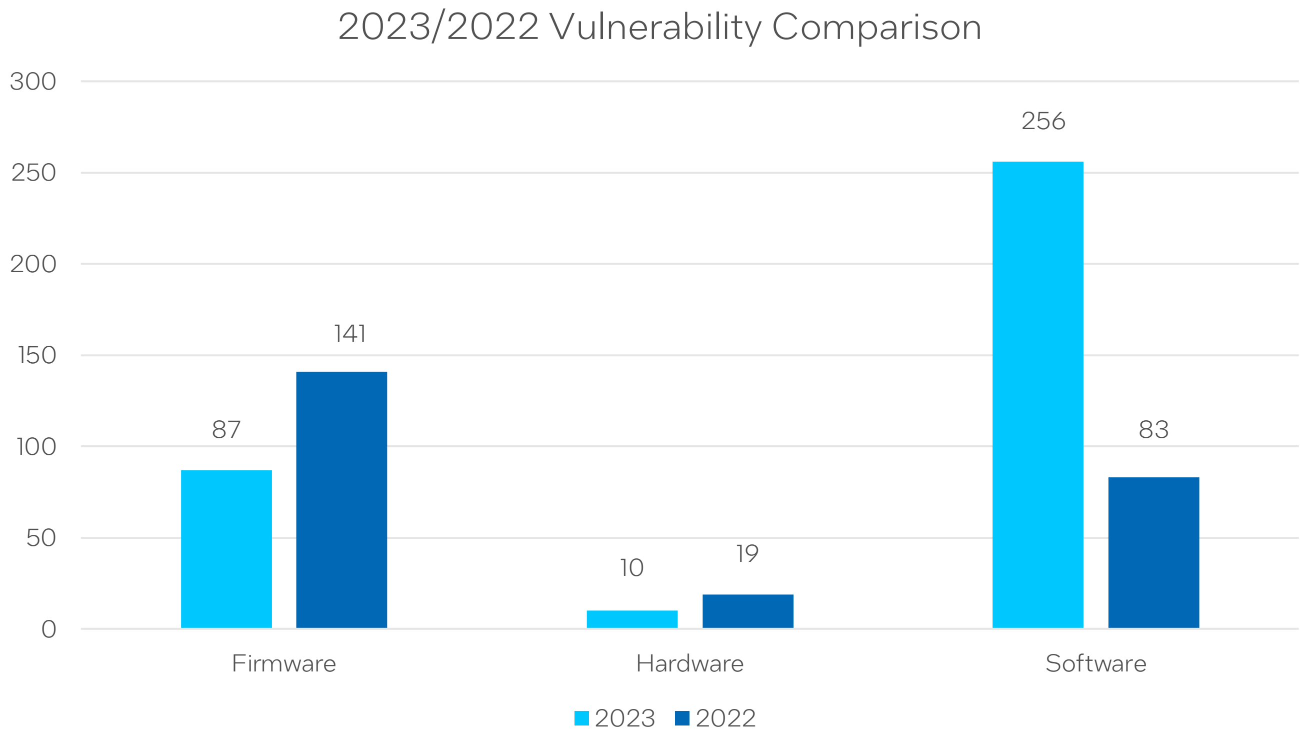
In 2023, Intel addressed 353 vulnerabilities.

- 256 vulnerabilities were in software, including applications, drivers, toolkits, SDKs, and utilities.
- 87 were discovered in firmware, including platform firmware, wireless and FPGA components, Intel NUC, SSDs, server boards, and other products.
- The remaining ten vulnerabilities were classified as hardware, 8 of which affected CPUs, with the other 2 affecting Intel Arc graphics cards.



Vulnerability Disclosures 2023 vs 2022

- There were 353 CVEs addressed in 2023 vs 243 in 2022 (a 45% increase).
- There were 38% fewer firmware vulnerabilities than in 2022.
- There were 47% fewer hardware vulnerabilities than in 2022.
- There were 208% more software vulnerabilities than in 2022, which were attributed to the growth of Intel's Bug Bounty and security researcher engagement programs.



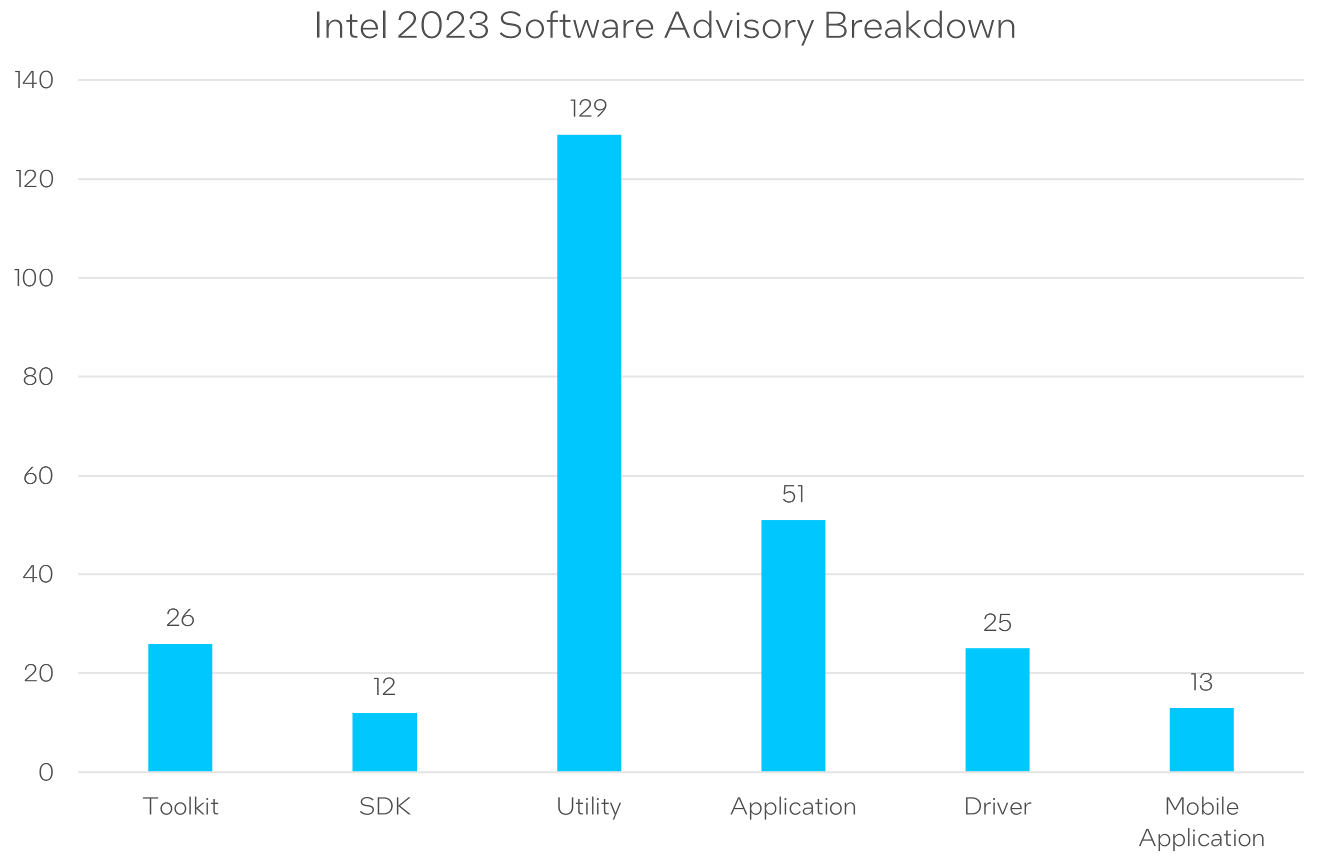
Bug bounties paid for software vulnerabilities increased by 104% over 2022.

Since 2018, there has been a 152% increase in the number of unique external security researchers engaged through Intel Bug Bounty Programs (page 23).

Further Breakdown of Intel Software Advisories

Intel is best known for building processors, but it is also a software and services company driving our software-defined, silicon-enhanced strategy. In 2023, 73% (256) of vulnerabilities addressed by Intel were in software. Here, we further break down the software category as follows:

- Toolkit (ex: Intel® oneAPI Toolkit)
- SDK (ex: Intel® SGX SDK)
- Utility (ex: firmware update utilities)
- Application (ex: Intel® Unite)
- Driver (ex: WiFi drivers)
- Mobile Application (ex: Intel® Smart Campus for Android)



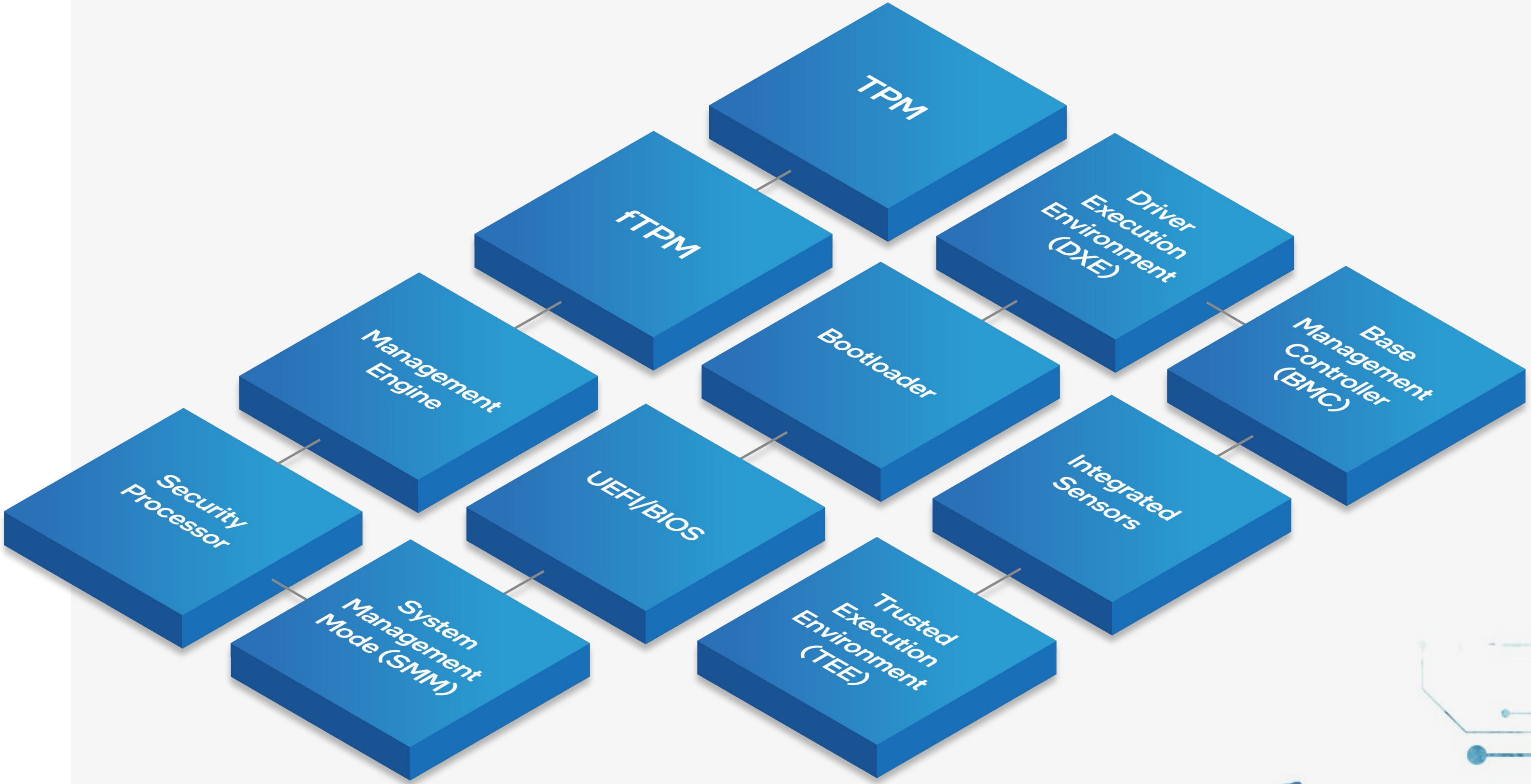
Intel - AMD Competitive Vulnerability Analysis

Platform Firmware

For the purposes of this competitive report, platform firmware is defined as firmware that maps to silicon and generally ships as part of a CPU/processor platform.

The boxes to the right are generic descriptions and represent just some of the components/features containing code that collectively represent platform firmware.

These examples also represent the types of firmware where vulnerabilities were disclosed in either Intel or AMD products.

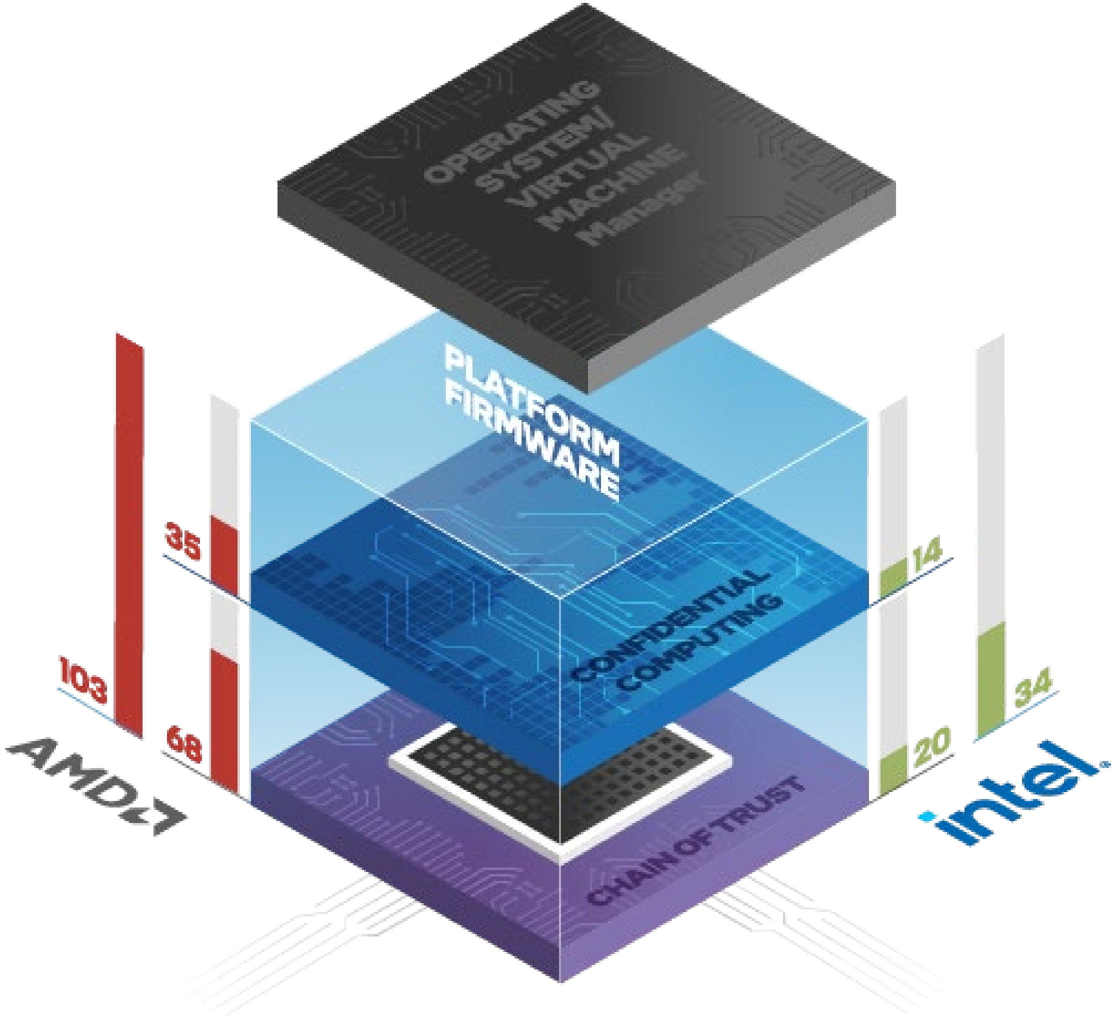

TPM
fTPM
Driver Execution Environment (DXE)
Management Engine
Bootloader
Base Management Controller (BMC)
Security Processor
UEFI/BIOS
Integrated Sensors
System Management Mode (SMM)
Trusted Execution Environment (TEE)

Platform Firmware Vulnerabilities

This analysis looks at vulnerabilities publicly disclosed by Intel and AMD during the calendar year 2023. This is the first full calendar year that comparable data is available, as **AMD did not start disclosing internally found vulnerabilities until May 2022.**

Given the importance of security starting at the hardware layer, we break out the data into these firmware categories:

1. Platform firmware totals
2. Chain of trust/secure boot features
3. Confidential computing features

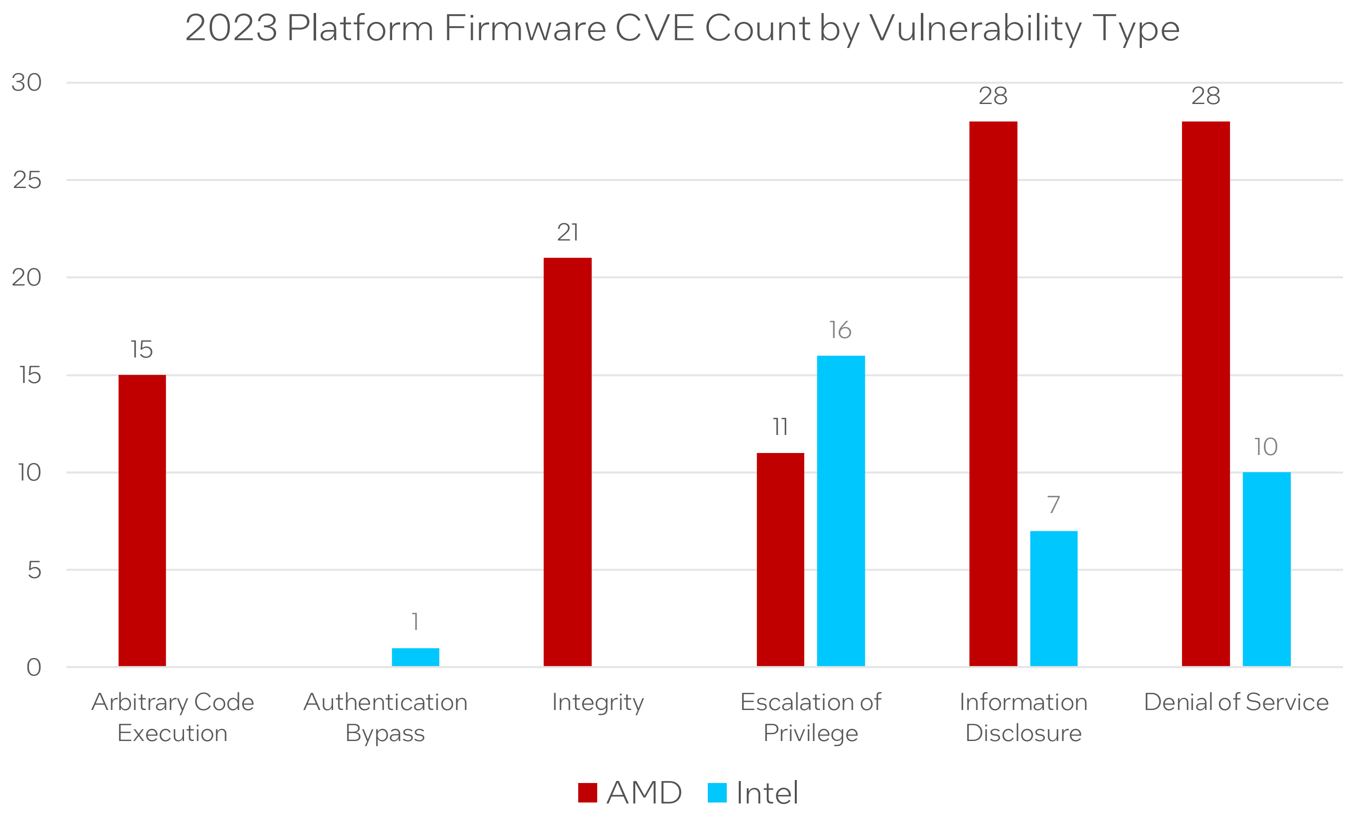


AMD had 3x more platform firmware vulnerabilities in 2023 than Intel.

Platform Firmware by Vulnerability Type

The vulnerability types listed in the chart at right represent those assigned to the CVEs in the publicly available data used to compile this report. For 2023, all Intel vulnerabilities were scored using the Common Vulnerability Scoring System (CVSS) version 3.1, and each CVE is published with a link to the CVSS 3.1 calculator to provide customers with more information for their threat assessments.

We could not confirm from AMD's website which CVSS scoring system they are using and found that AMD does not consistently provide the numerical CVSS score in their advisories.



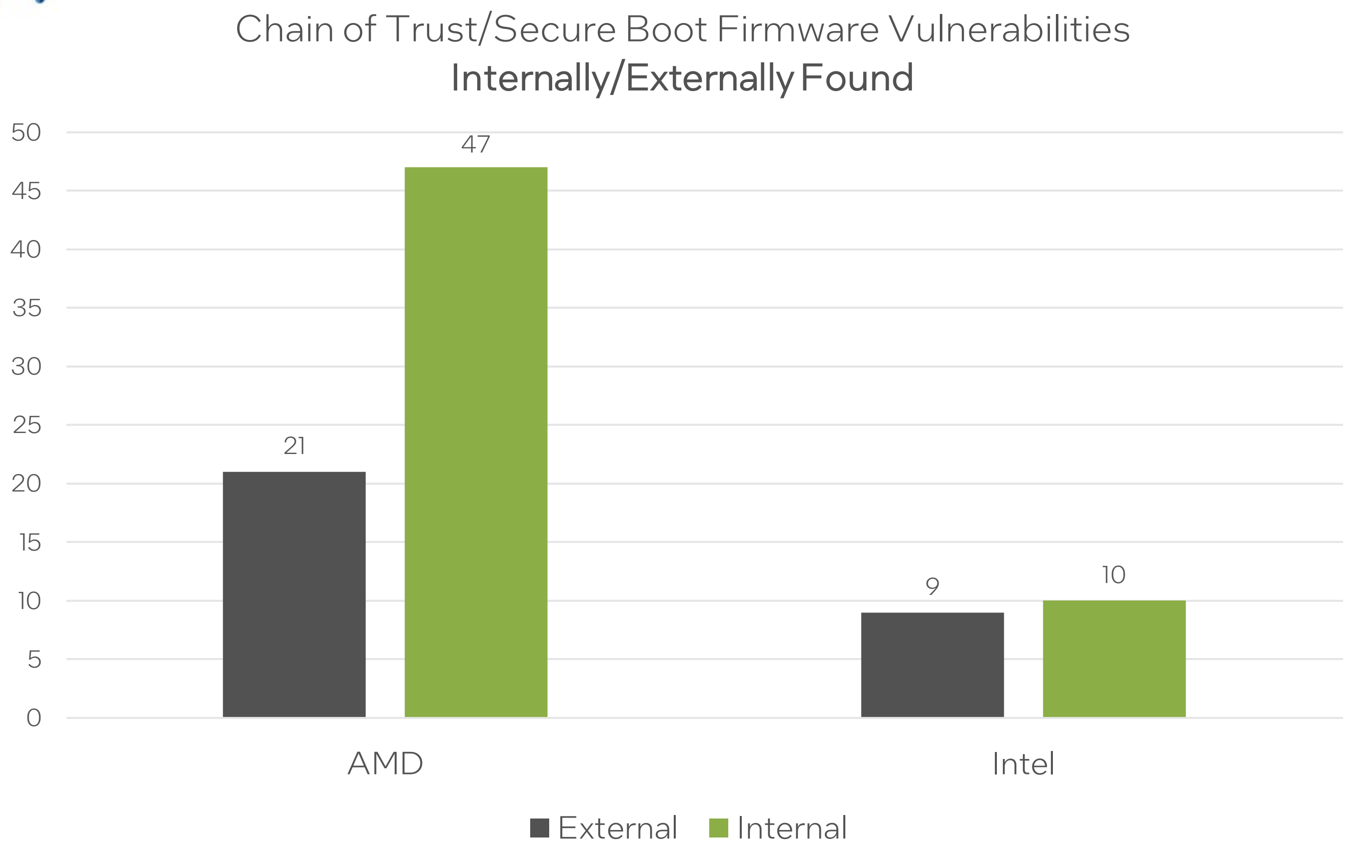
35% of AMD platform firmware vulnerabilities were Arbitrary Code Execution or Integrity issues.

Chain of Trust/ Secure Boot Firmware

The hardware chain of trust refers to a chain of events that ensures a computer boots with verified code. Each link in the chain is verified and measured before that component is loaded. Thus, the system's overall security relies on the components and features that make up the chain of trust.

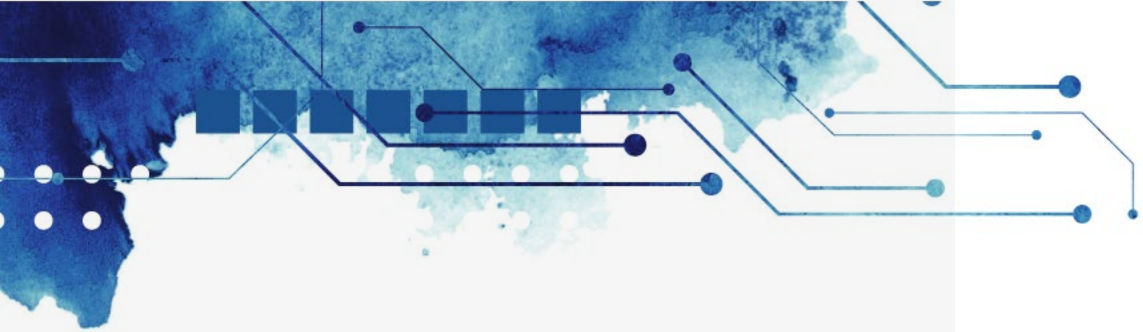
Examples of such components include the Intel Converged Security and Management Engine (Intel® CSME) and AMD Secure Processor, which are dedicated security processors validating code before execution.

The hardware chain of trust is the first critical step in system security and helps ensure the validity of confidential computing features that run on top of it.



In 2023, AMD had over 3.5x as many vulnerabilities in their Chain of Trust/Secure Boot firmware components and features than Intel.

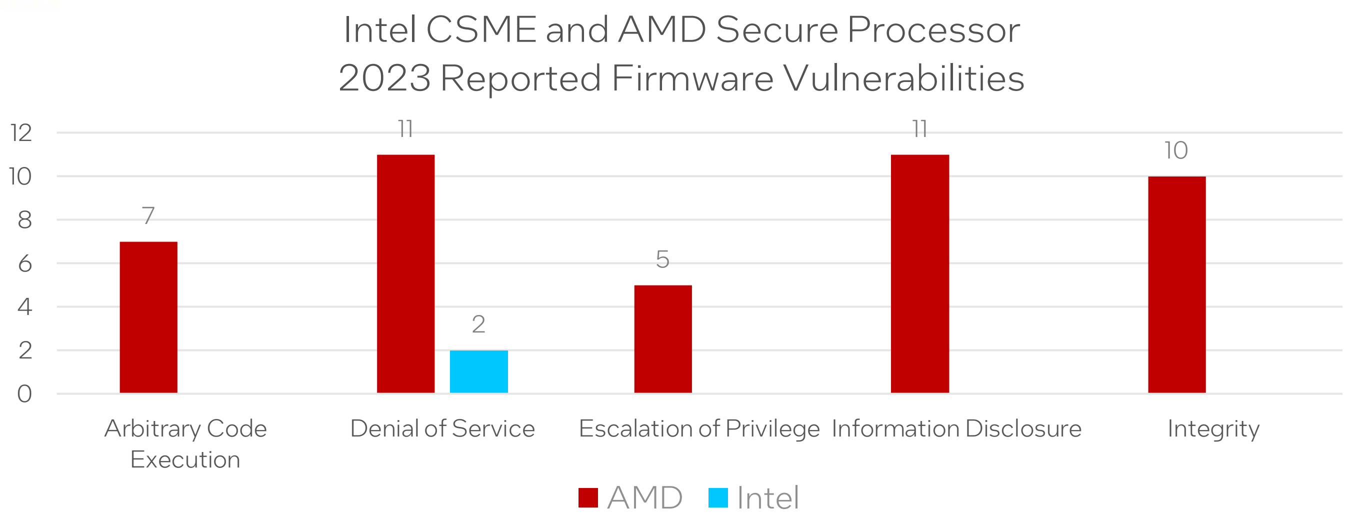
Intel found 53% of Chain of Trust/Secure Boot firmware vulnerabilities internally in 2023, while AMD found 69%.



Intel and AMD Security Processors

The Intel® Converged Security and Management Engine (CSME) and the AMD Secure Processor (ASP) are dedicated security processors responsible for the hardware root of trust. As the first step in the chain of trust, these components are responsible for validating the first firmware code to load in the boot process.

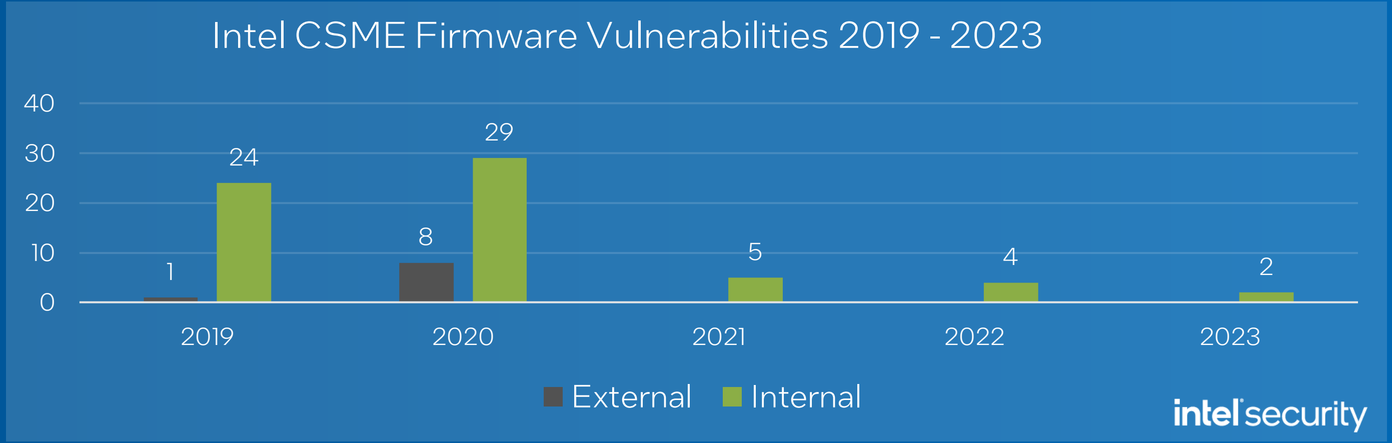
Vulnerabilities in the root of trust can potentially compromise the entire system and make confidential computing solutions unreliable.


Intel CSME and AMD Secure Processor 2023 Reported Firmware Vulnerabilities

In 2023, AMD reported 22x more firmware vulnerabilities in ASP than were discovered in Intel CSME.

Results!

The impact of Intel's product security assurance efforts and the maturity level of processes are represented in the downward trend in vulnerabilities discovered in Intel CSME. Additionally, architectural hardening and added layers of protection make CSME resistant to attack even if vulnerabilities are discovered.


Intel CSME Firmware Vulnerabilities 2019 - 2023

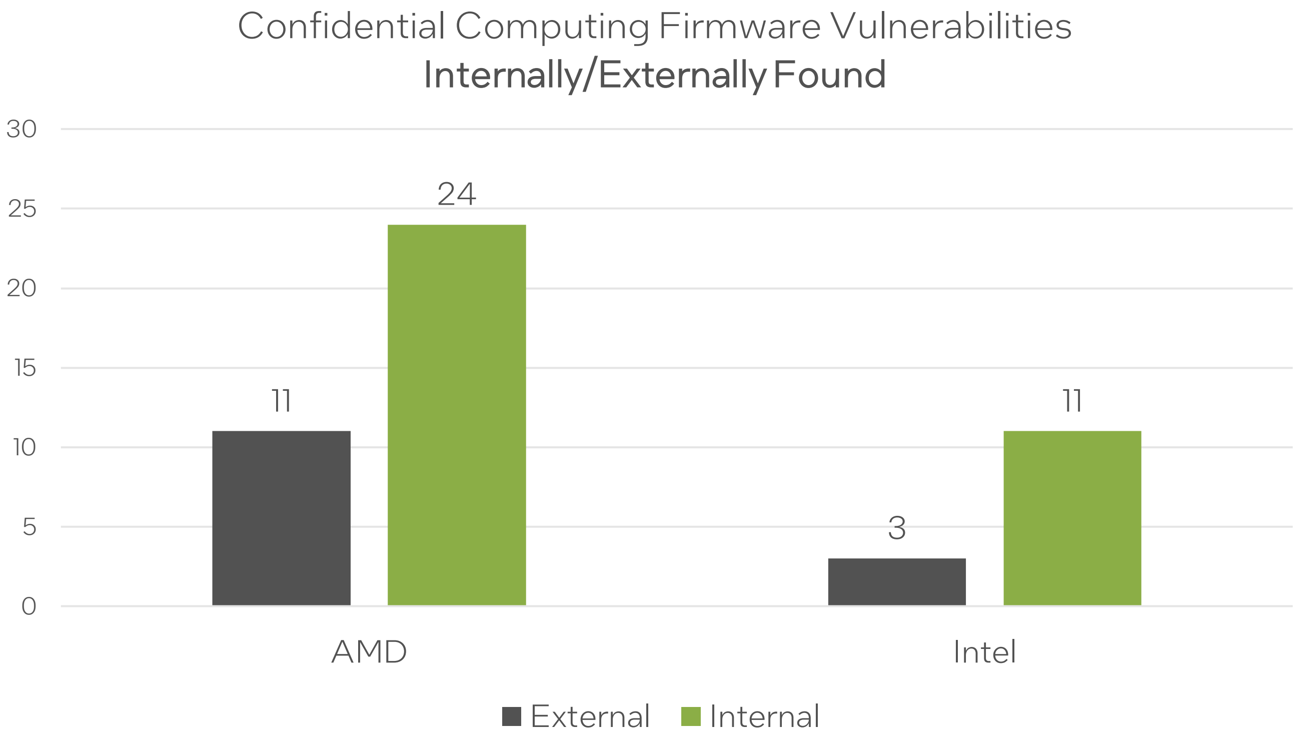
Confidential Computing Firmware

Confidential computing is the protection of data in use by performing computation in a hardware-based, attested Trusted Execution Environment.

CONFIDENTIAL COMPUTING TECHNOLOGIES

Intel: Intel® Trust Domain Extensions (Intel® TDX) and Intel® Software Guard Extensions (Intel® SGX).

AMD: Secure Encrypted Virtualization (SEV), SEV-ES (Encrypted State), and SEV-SNP (Secure Nested Pages).



In 2023, AMD reported 2.5x as many vulnerabilities in their confidential computing firmware components and features than Intel.

Intel found 79% of confidential computing firmware vulnerabilities internally in 2023, while AMD found 69%.

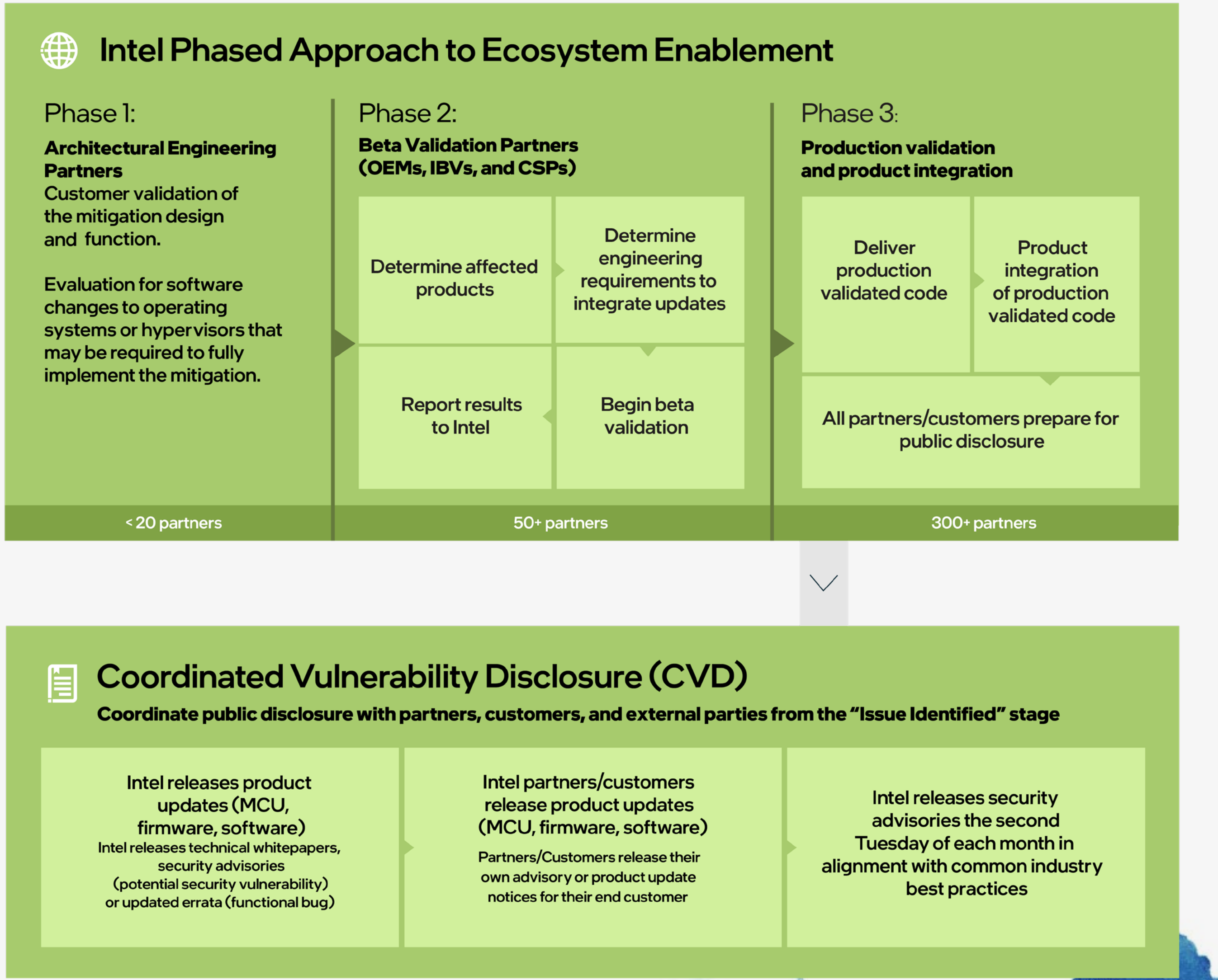
Coordinating Disclosures Across the Ecosystem

Industry-Leading Intel Platform Update Process

Platform firmware updates require coordination with a large ecosystem of partners, including independent BIOS vendors (IBVs), original device manufacturers (ODMs), original equipment manufacturers (OEMs), operating system and hypervisor vendors, and cloud service providers (CSPs).

Designed with input from these partners, **the Intel Platform Update (IPU) process provides a predictable quarterly cadence** of updates that enables planning and efficient use of validation resources across the partner ecosystem **and helps ensure that all customers receive high-quality updates for all supported products at the time vulnerabilities are publicly disclosed**.

Click here to view the full Intel Platform Update process diagram.



Intel Phased Approach to Ecosystem Enablement

Phase 1:

Architectural Engineering Partners

Customer validation of the mitigation design and function.

Evaluation for software changes to operating systems or hypervisors that may be required to fully implement the mitigation.

< 20 partners

Phase 2:

Beta Validation Partners (OEMs, IBVs, and CSPs)

Determine affected products

Determine engineering requirements to integrate updates

Begin beta validation

Report results to Intel

50+ partners

Phase 3:

Production validation and product integration

Deliver production validated code

Product integration of production validated code

All partners/customers prepare for public disclosure

300+ partners

Coordinated Vulnerability Disclosure (CVD)

Coordinate public disclosure with partners, customers, and external parties from the "Issue Identified" stage

Intel releases product updates (MCU, firmware, software)
Intel releases technical whitepapers, security advisories (potential security vulnerability) or updated errata (functional bug)

Intel partners/customers release product updates (MCU, firmware, software)
Partners/Customers release their own advisory or product update notices for their end customer

Intel releases security advisories the second Tuesday of each month in alignment with common industry best practices

Intel Bug Bounty Programs

Intel Bug Bounty Programs

Defending against ongoing cybersecurity threats is a task for every company in the tech supply chain, helped by the valuable contributions of ethical hackers and security researchers across the industry.

We value the contributions from the community, knowing they help us improve the security of our products, ultimately improving defenses for our customers. Therefore, we believe in paying bounties and offering a proactive program with live hacking events to better collaborate with the ethical hacking community to find bugs before threat actors discover them.

Project Circuit Breaker

Under the Intel® Bug Bounty Program, Project Circuit Breaker is tasked with building a community of ethical hackers around Intel technologies and creating live hacking events that bring that community together with Intel engineers to collaborate on hunting bugs.

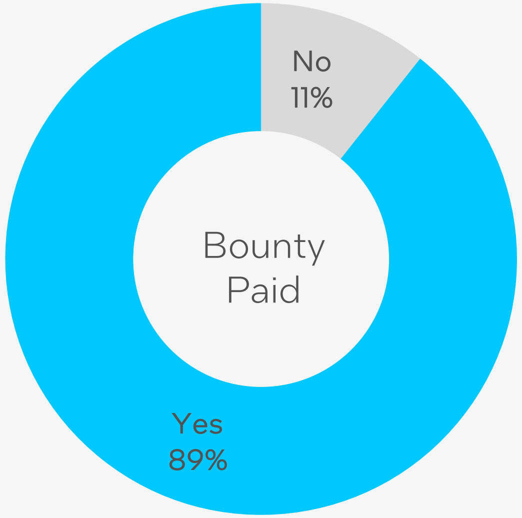
The latest challenge, Knights of Elektron, invited 88 elite hackers to target Intel's latest Software-as-a-Service (SaaS) product.

The challenge kicked off virtually, where the group was trained on the technology, event scope, and bug hunt rules. Then, hackers worldwide flew into Lisbon; some even self-funded the trip for the value they saw in the opportunity to network, learn, and share their expertise. For 16 days, the community scoured the software for bugs.

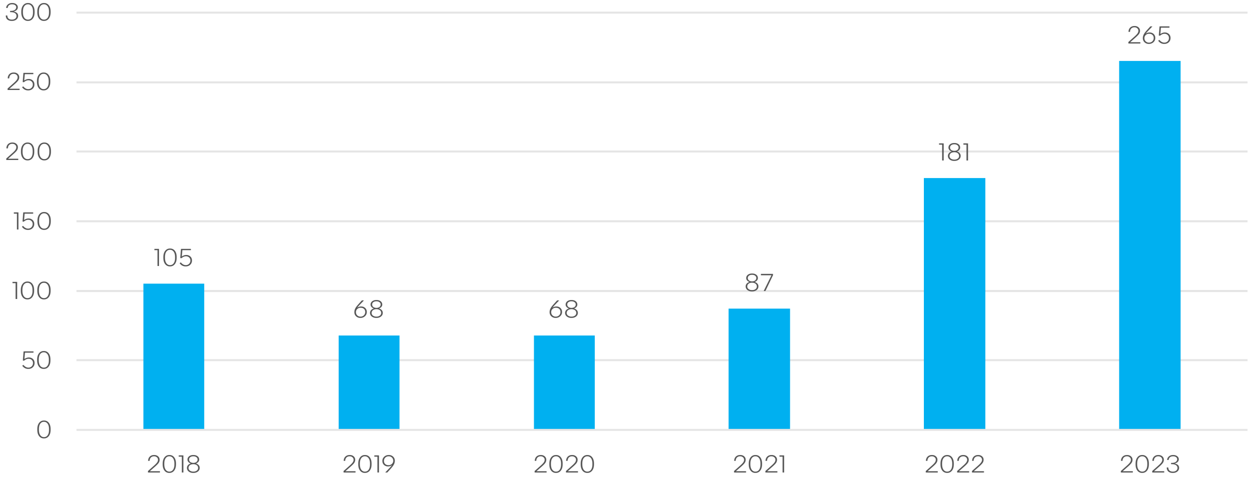
By the end of the event, we had received 428 submissions encompassing 75 unique vulnerabilities. Those findings allow us to focus on the issues where we can improve product security, making the product more resilient to attacks.

Intel Bug Bounty Programs

In 2023, 89% of CVEs reported by external sources qualified for a bounty.



Unique Researchers Engaged in Intel Bug Bounty



What Participants Had to Say About the Knights of Elektron Event

"The experience of learning the technology that we're getting now is going to pay off in the next event and the next time we interact with this service."

Garret Adler
Security Researcher

"The pressure is definitely there. It's a pretty small application. There's a lot of hackers and it's a very challenging concept."

Justin Gardner
Security Researcher

"Running with Intel as a target was, in this case, extremely challenging."

Frans Rosén
Security Researcher

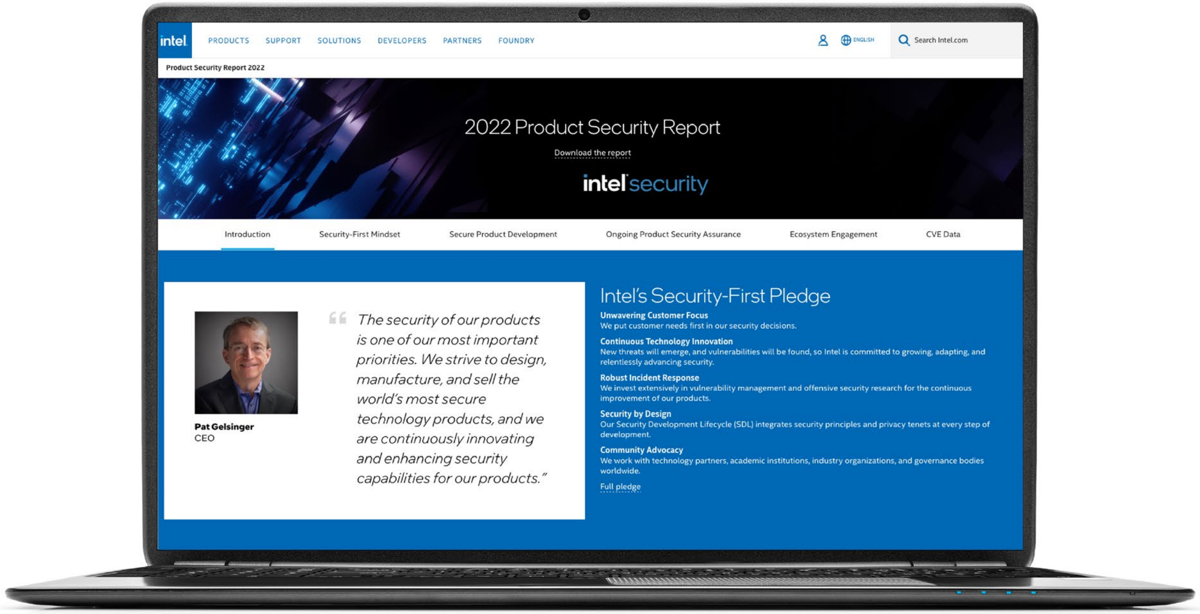
Reference

Previous Intel Product Security Reports

Intel's approach to product security assurance includes:

- A security-first mindset/culture
- Secure product development
- Ongoing product security assurance
- Ecosystem engagement

For an in-depth review, please visit the Intel Product Security Assurance website.



Product Security Report 2022

2022 Product Security Report

Download the report

intel security

Introduction | Security-First Mindset | Secure Product Development | Ongoing Product Security Assurance | Ecosystem Engagement | CVE Data

"The security of our products is one of our most important priorities. We strive to design, manufacture, and sell the world's most secure technology products, and we are continuously innovating and enhancing security capabilities for our products."

Pat Gelsinger
CEO

Intel's Security-First Pledge

Unwavering Customer Focus
We put customer needs first in our security decisions.

Continuous Technology Innovation
New threats will emerge, and vulnerabilities will be found, so Intel is committed to growing, adapting, and relentlessly advancing security.

Robust Incident Response
We invest extensively in vulnerability management and offensive security research for the continuous improvement of our products.

Security by Design
Our Security Development Lifecycle (SDL) integrates security principles and privacy tenets at every step of development.

Community Advocacy
We work with technology partners, academic institutions, industry organizations, and governance bodies worldwide.

Full pledge

2019 PRODUCT SECURITY REPORT
Intel Product Assurance and Security

Platform Firmware Data Sources

These publicly available advisories/bulletins represent the source data for the competitive analysis.

Click on the company names below to find their respective public security advisories/bulletins.

AMD

Advisory ID	Title	Release Date
AMD-SB-1031	AMD Client Vulnerabilities – January 2023	1/10/2023
AMD-SB-1032	AMD Server Vulnerabilities – January 2023	1/10/2023
AMD-SB-1045	Cross-Thread Return Address Predictions	2/14/2023
AMD-SB-3001	AMD Server Vulnerabilities – May 2023	5/9/2023
AMD-SB-3004	AMD SEV VM Power Side Channel Security Bulletin	7/11/2023
AMD-SB-3005	AMD INVD Instruction Security Vulnerability	11/14/2023
AMD-SB-4001	Client Vulnerabilities – May 2023	5/9/2023
AMD-SB-4002	AMD Client Vulnerabilities – November 2023	11/14/2023
AMD-SB-4003	SMM Memory Corruption Vulnerability	8/8/2023
AMD-SB-4005	fTPM Voltage Fault Injection	8/8/2023
AMD-SB-4007	DXE Driver Memory Leaks	9/20/2023
AMD-SB-6003	AMD Graphics Driver Vulnerabilities – November 2023	11/14/2023
AMD-SB-7002	TPM Out of Bounds Access	4/11/2023
AMD-SB-7005	Return Address Security Bulletin	8/8/2023
AMD-SB-7006	Software based Power Side Channel on AMD CPUs	8/1/2023
AMD-SB-7007	Speculative Leaks Security Notice	8/8/2023
AMD-SB-7008	Cross-Process Information Leak	7/24/2023
AMD-SB-7011	AMD SMM Supervisor Vulnerability Security Notice	11/14/2023

Intel

Advisory ID	Title	Release Date
INTEL-SA-00700	2023.1 IPU - Intel® Atom® and Intel® Xeon® Scalable Processors Advisory	2/14/2023
INTEL-SA-00717	2023.1 IPU - BIOS Advisory	2/14/2023
INTEL-SA-00718	2023.1 IPU - Intel® Chipset Firmware Advisory	2/14/2023
INTEL-SA-00721	Intel® Integrated Sensor Solution Advisory	2/14/2023
INTEL-SA-00730	3rd Generation Intel® Xeon® Scalable Processors Advisory	2/14/2023
INTEL-SA-00737	Integrated BMC and OpenBMC Firmware Advisory	2/14/2023
INTEL-SA-00738	2023.1 IPU - Intel® Xeon® Processor Advisory	2/14/2023
INTEL-SA-00767	2023.1 IPU - Intel® Processor Advisory	2/14/2023
INTEL-SA-00807	2023.2 IPU – BIOS Advisory	5/9/2023
INTEL-SA-00783	2023.3 IPU - Intel® Chipset Firmware Advisory	8/8/2023
INTEL-SA-00813	2023.3 IPU - BIOS Advisory	8/8/2023
INTEL-SA-00828	2023.3 IPU - Intel® Processor Advisory	8/8/2023
INTEL-SA-00836	2023.3 IPU - Intel® 3rd Gen Intel® Xeon® Scalable processors Advisory	8/8/2023
INTEL-SA-00837	2023.3 IPU - Intel® Xeon® Processor Advisory	8/8/2023
INTEL-SA-00924	2023.4 IPU - BIOS Advisory	11/14/2023
INTEL-SA-00950	2023.4 IPU Out-of-Band (OOB) - Intel® Processor Advisory	11/14/2023

intel security

Notices & Disclaimers

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 does not control or audit third-party data. You should consult other sources to evaluate accuracy.