
intel security
2024 Intel Product
Security Report

Table of Contents

Introduction

Security Starts with Intel

Intel technology is designed to accelerate a Zero Trust strategy, enabling hardware as the root of trust, with industry-leading security assurance as the foundation everything is built on.

A 2024 independent study by ABI Research[1] offers a comparative assessment of the Security Assurance Practices of top silicon vendors, ranking Intel number one in the industry.

Product security assurance at Intel is an investment in people, processes, and tools extending from development and manufacturing to the end of the product lifecycle. It means that customers can be confident in Intel's Security-First Pledge: we design with security in mind, continually look for ways to strengthen our products, and disclose vulnerabilities we find. Working with our customers and industry partners, we can achieve the secure performance people expect and deliver technology they trust.

This report provides a transparent analysis of the product vulnerabilities Intel disclosed in 2024. 96% of these were the result of Intel's proactive product security assurance efforts, through which Intel actively looks for and resolves potential vulnerabilities before they are publicly known.

The report also provides evidence to support the findings by ABI Research by comparing publicly disclosed platform firmware and Graphics Processing Unit (GPU) vulnerabilities with those reported by some of our competition. The goal is not to compare vulnerability counts but to look deeper at the types of vulnerabilities and the foundational technologies they impact.

[1] As measured by ABI Research

Our Roadmap is Aligned to Zero Trust Principles

Intel technologies help you build a Zero Trust strategy, establishing hardware as the root of trust

Endpoint Security

Strengthen defenses with AI-powered threat detection, insights, and hardware-based security measures

Network Security

Connect people with the resources they need through encryption-based identity and access control

Information & Data Security

Designed to isolate and protect your sensitive data while in use to enhance confidentiality, integrity, and availability

Physical Security

Help prevent real-world attacks by managing the convergence of AI, physical, and cyber security assets

Product Security Assurance: Built on a Foundation of Trust

Choose products designed with security in mind, backed by the industry's best security assurance[1]

Security Assurance Practices[1]

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

Intel's proactive product security assurance efforts account for

96% of vulnerabilities

disclosed in 2024.

About This Report

The assessment of security vulnerabilities is an ongoing part of Intel's silicon industry-leading product security assurance. This end-of-year report is intended to provide transparency in alignment with Intel's Security-First Pledge.

This 6th annual Intel Product Security Report provides an analysis of the vulnerabilities Intel publicly disclosed in the calendar year 2024.

2024 Key Points:

- 96% of the vulnerabilities addressed were discovered through Intel's proactive product security assurance efforts.
- 100% of the Intel processor vulnerabilities addressed were discovered through internal security research.
- 53% of the 374 vulnerabilities Intel addressed received a bug bounty payment.
- 84% of the bug bounties paid were in the software category.
- AMD reported 4.4x more firmware vulnerabilities in their hardware root-of-trust than Intel.
- AMD reported 1.8x more firmware vulnerabilities in their confidential computing technologies than Intel.
- In the GPU category, NVIDIA had only high-severity vulnerabilities (18) in 2024.

Competitive Assessment

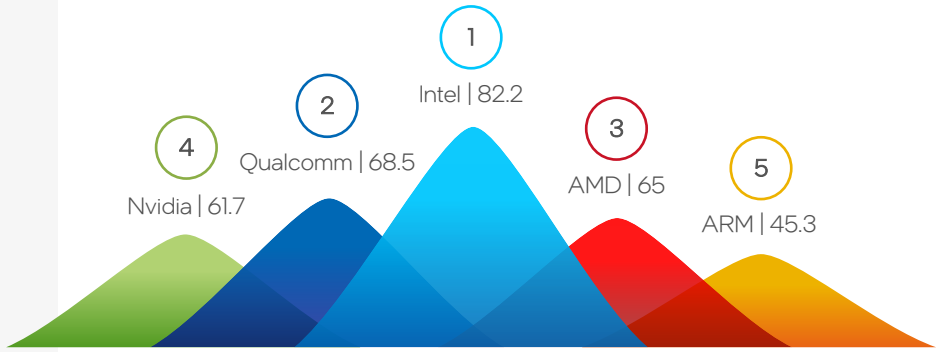
When it comes to silicon, purchasing decisions are largely based on price, performance, and power consumption, with the latter two contributing heavily to the total cost of ownership over the lifetime of the product.

Total cost of ownership also includes servicing, which is the cost of deploying security updates. Applying security updates is, in essence, a cost-avoidance activity. For example, in 2024, the global average cost of a data breach was $4.48M[1] and applying security updates is an effort to help avoid such costs.

Intel invests heavily in security technologies and security assurance and the competitive assessment in this report looks at common platform firmware and graphics processing unit (GPU) vulnerabilities as a comparative analysis of product security assurance results.

Security starts with silicon. Choose the silicon designed and supported by the best security assurance in the industry.

Intel Ranked #1 vs. Key Competitors for Product Security Assurance[2]



Areas of Intel leadership:

- Security Development Lifecycle
- Proactive Security Practices
- Thread Discovery and Response
- Offensive Security Research
- Security Training
- Community Engagement

To learn more about Intel's differentiating product security assurance investments, visit: https://www.intel.com/content/www/us/en/security/product-security-assurance.html

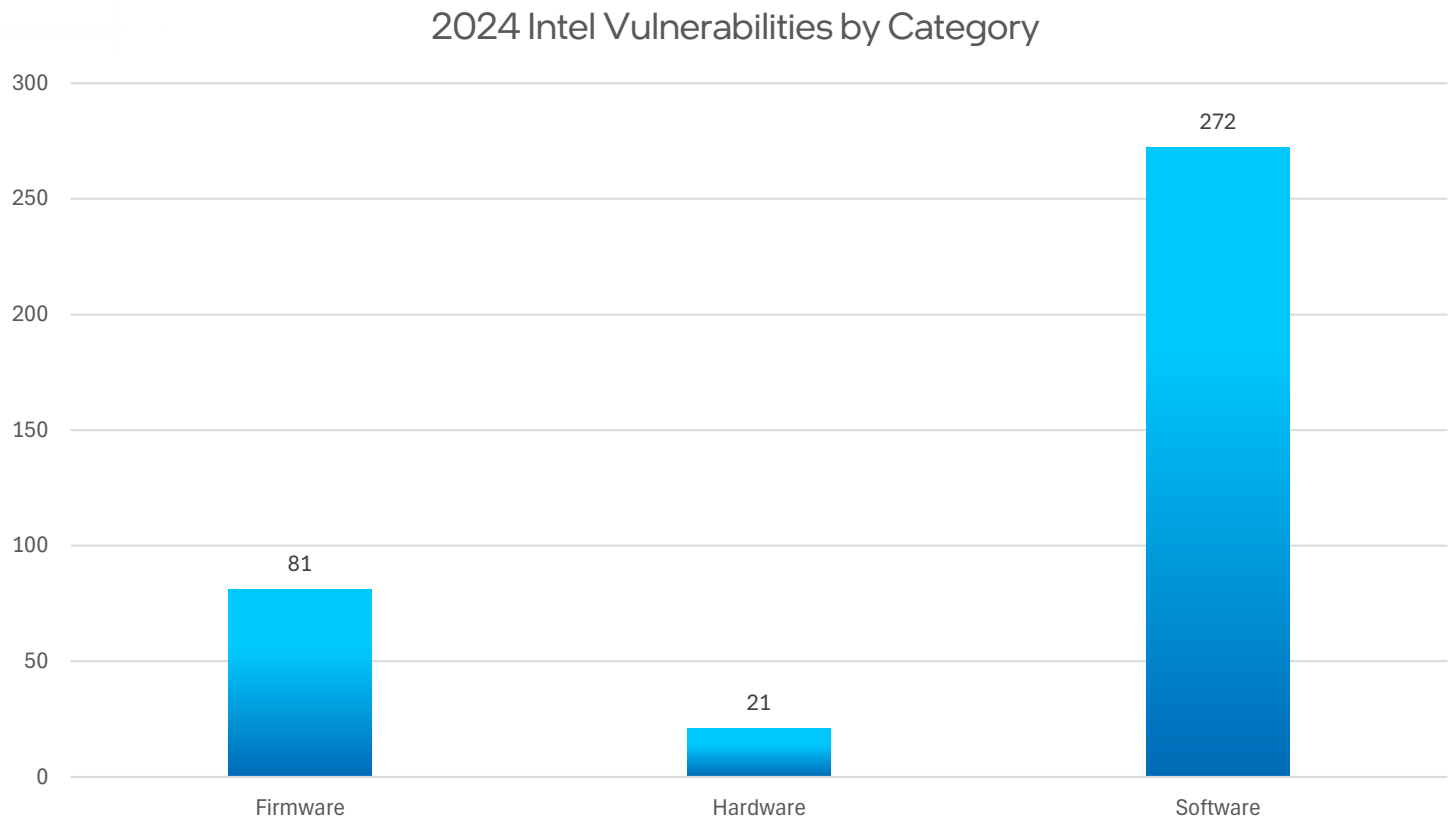
[1] IBM, Cost of a Data Breach Report 2024
[2] As measured by ABI Research

Summary of Intel 2024 Vulnerabilities

Summary of Intel 2024 Vulnerabilities

In 2024, Intel addressed 374 vulnerabilities.

- 272 vulnerabilities were in software, including applications, drivers, toolkits, SDKs, and utilities.
- 81 were discovered in firmware, including platform firmware, wireless and FPGA components, Intel NUC, SSDs, server boards, and other products.
- The remaining 21 vulnerabilities were classified as hardware vulnerabilities, all found internally by Intel researchers.

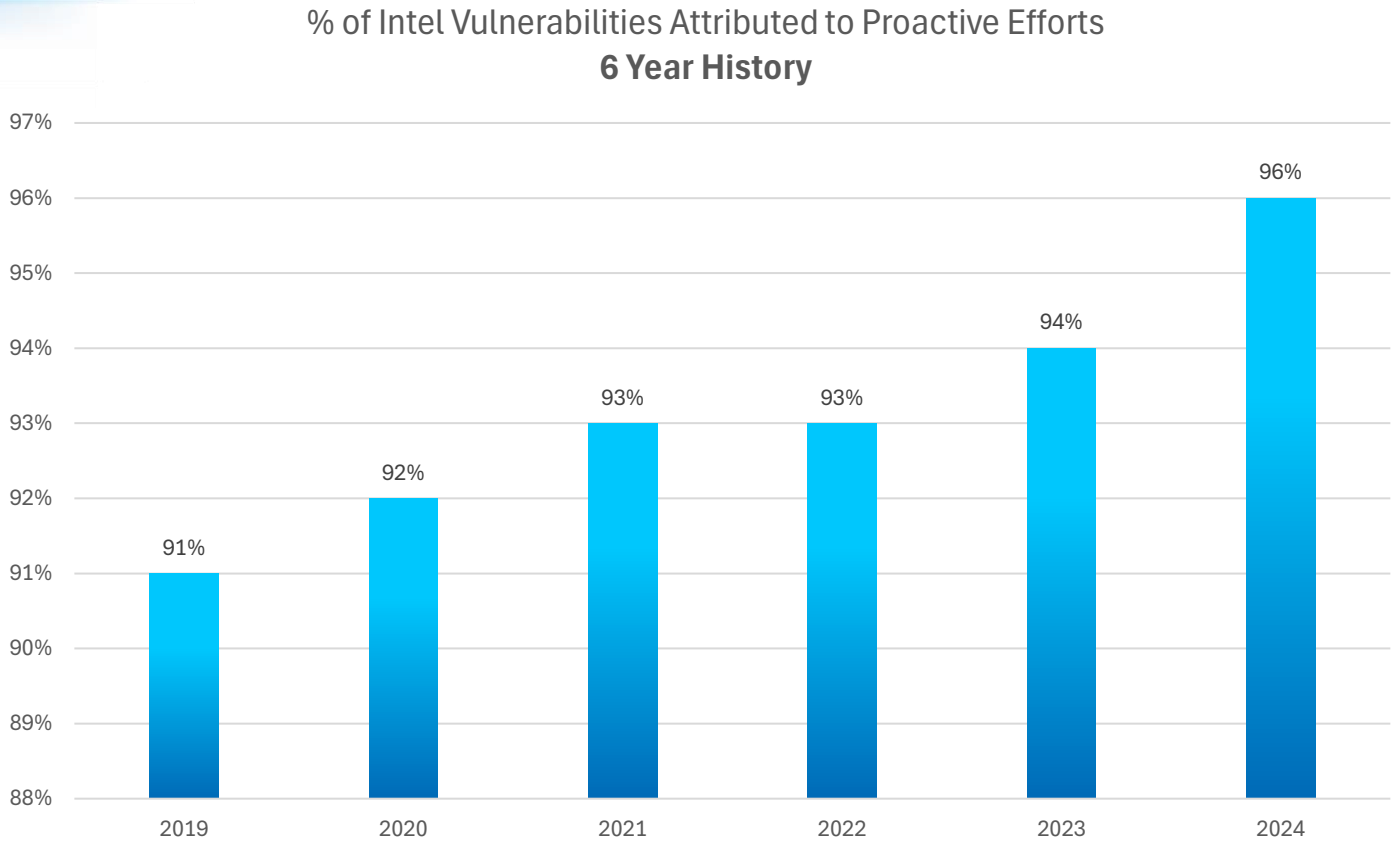


In 2024, 100% of hardware vulnerabilities were discovered internally by Intel employees.

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.

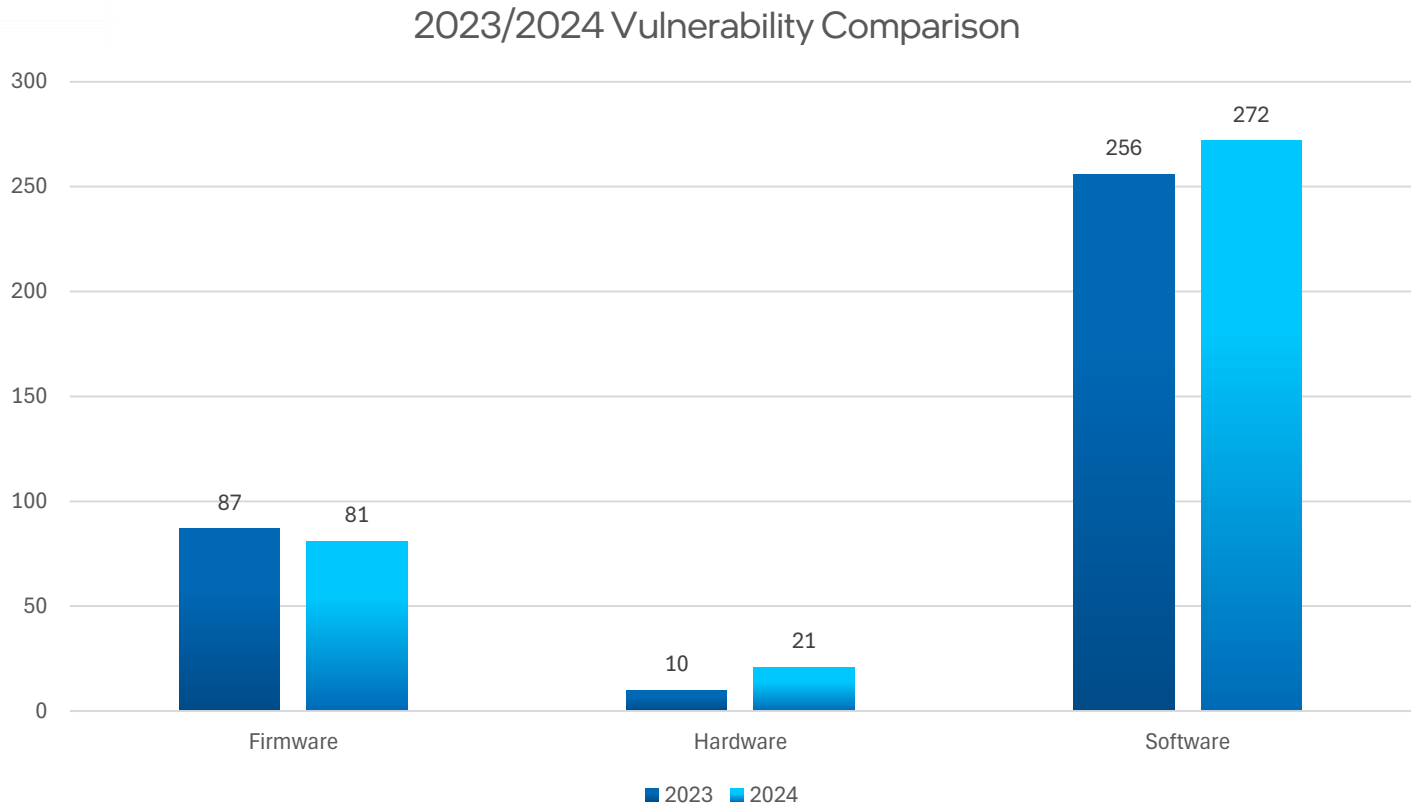
In 2024, the remaining 4% of vulnerabilities addressed by Intel were either not submitted through the Intel Bug Bounty program or were submitted by partners or other organizations that do not seek bounty payments. In all cases, Intel worked with researchers to coordinate the public disclosure of these issues meaning mitigations were available to customers on the public disclosure date.



In 2024, Intel's investment in proactive product security assurance accounted for 96% of the vulnerabilities discovered and mitigated.

Vulnerability Disclosures 2024 vs. 2023

- There were 374 CVEs addressed in 2024 vs. 353 in 2023 (a 6% increase).
- 100% of the hardware vulnerabilities addressed in 2024 were found internally by Intel researchers.
- In 2023, Intel's proactive efforts resulted in the discovery and mitigation of 92% of platform firmware vulnerabilities and 94% in 2024.

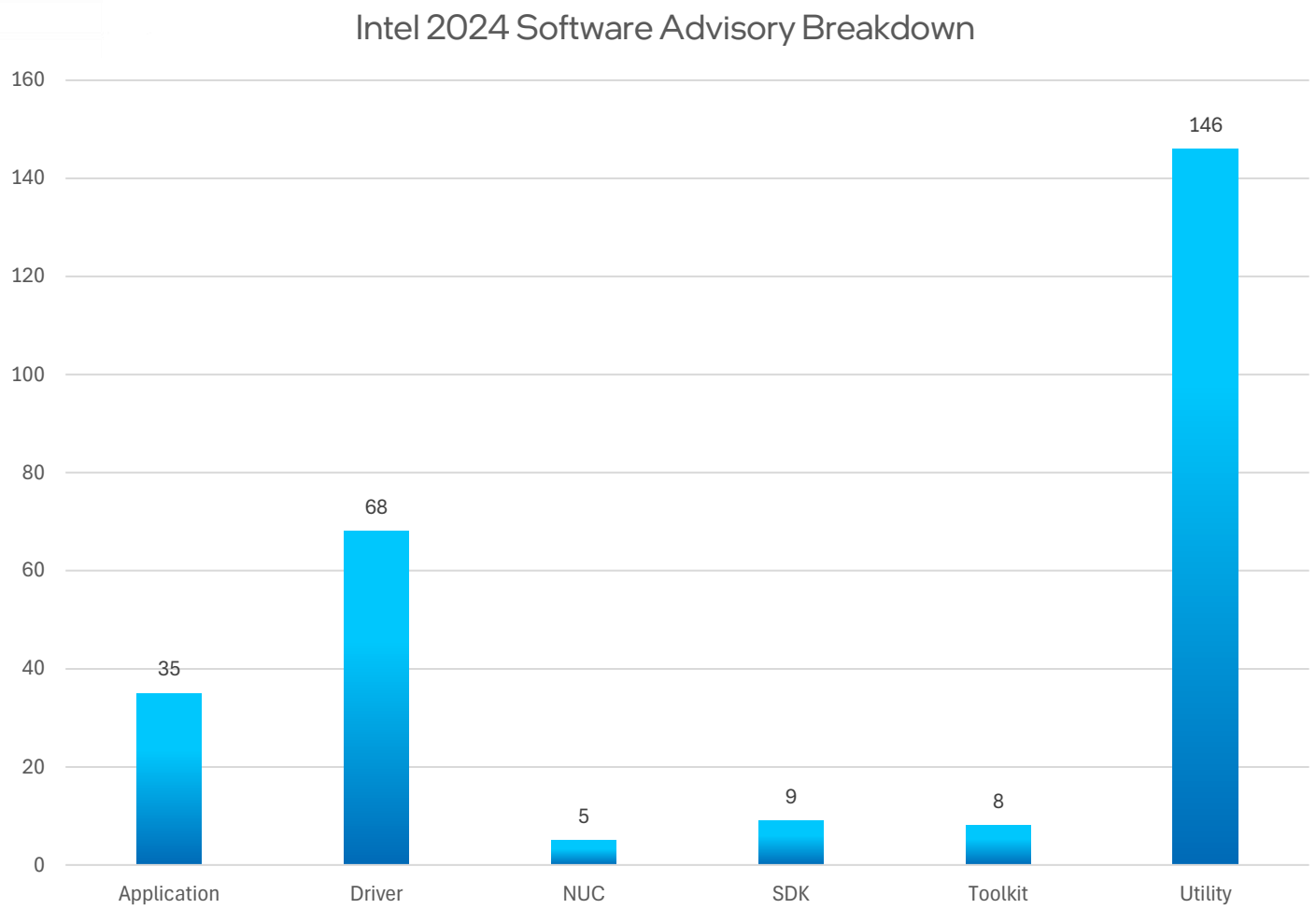


The firmware and software categories remained relatively flat, while Intel's internal product security assurance efforts accounted for 100% of the hardware issues addressed in 2024.

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 2024, 68% (272) of vulnerabilities addressed by Intel were in software. 92% of these were found and addressed as part of Intel's proactive efforts. Here, we further break down the software category as follows:

- Toolkit (ex: Intel® oneAPI Toolkit)
- Software Development Kit (ex: Intel® SGX SDK)
- Utility (ex: firmware update utilities)
- Application (ex: Intel® Neural Compressor)
- Driver (ex: Wi-Fi drivers)

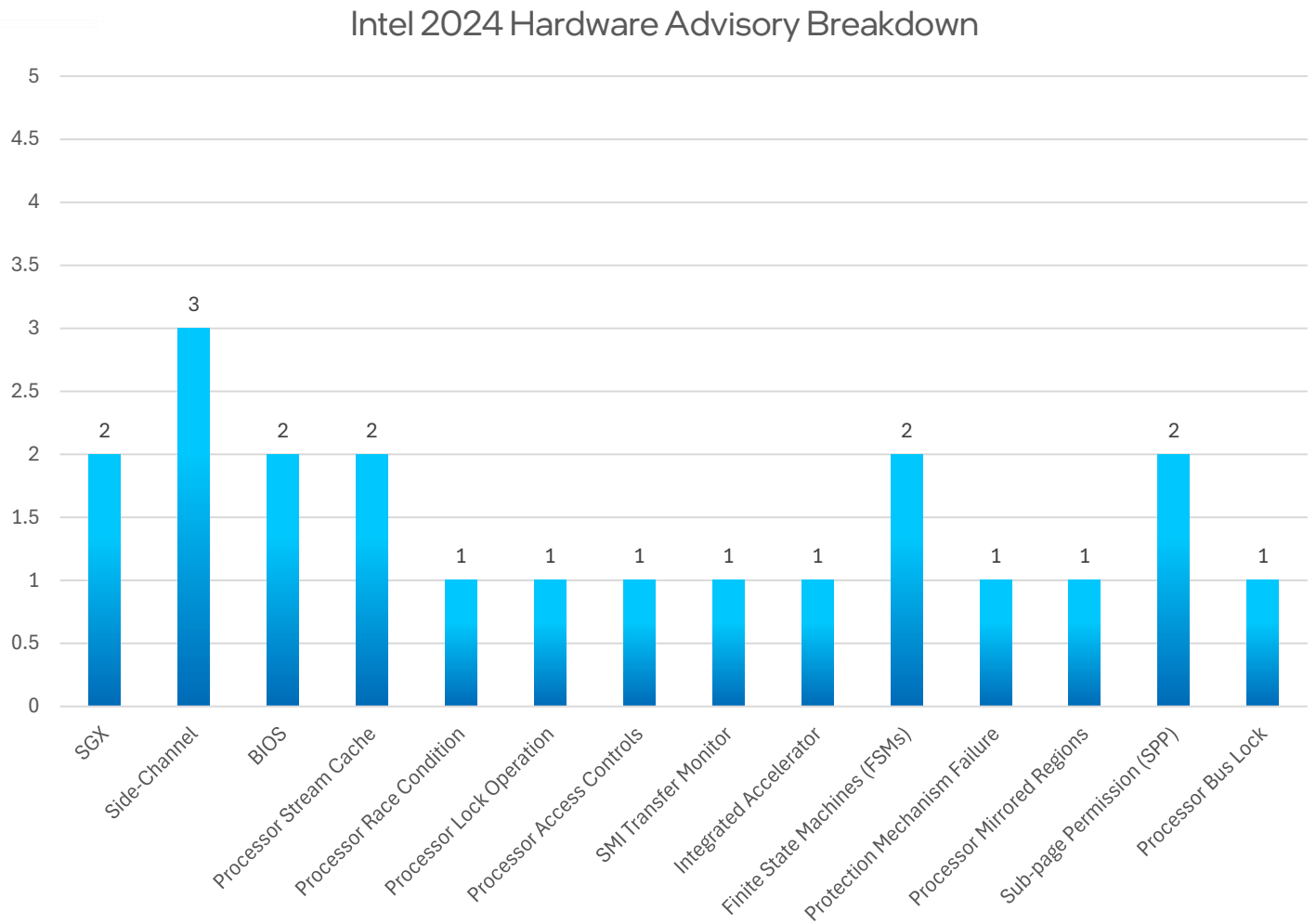


Further Breakdown of Intel Hardware Advisories

In 2024, 21 CVEs were in the Hardware category. **100% of these issues were discovered internally and mitigated by Intel.**

Further breakdown:

- **Processor:** Mitigations are typically delivered through BIOS firmware updates made available by systems manufacturers.
- **Intel SGX:** Confidential Computing technologies from Intel are continuously reviewed by internal researchers as well as through collaboration with industry partners such as Google and Microsoft.
- **Side-Channel:** In 2024, Intel provided mitigations for three internally found side-channel issues. Most external side-channel research in 2024 was focused on existing attack vectors such as Spectre v2, which are addressed by existing mitigations.



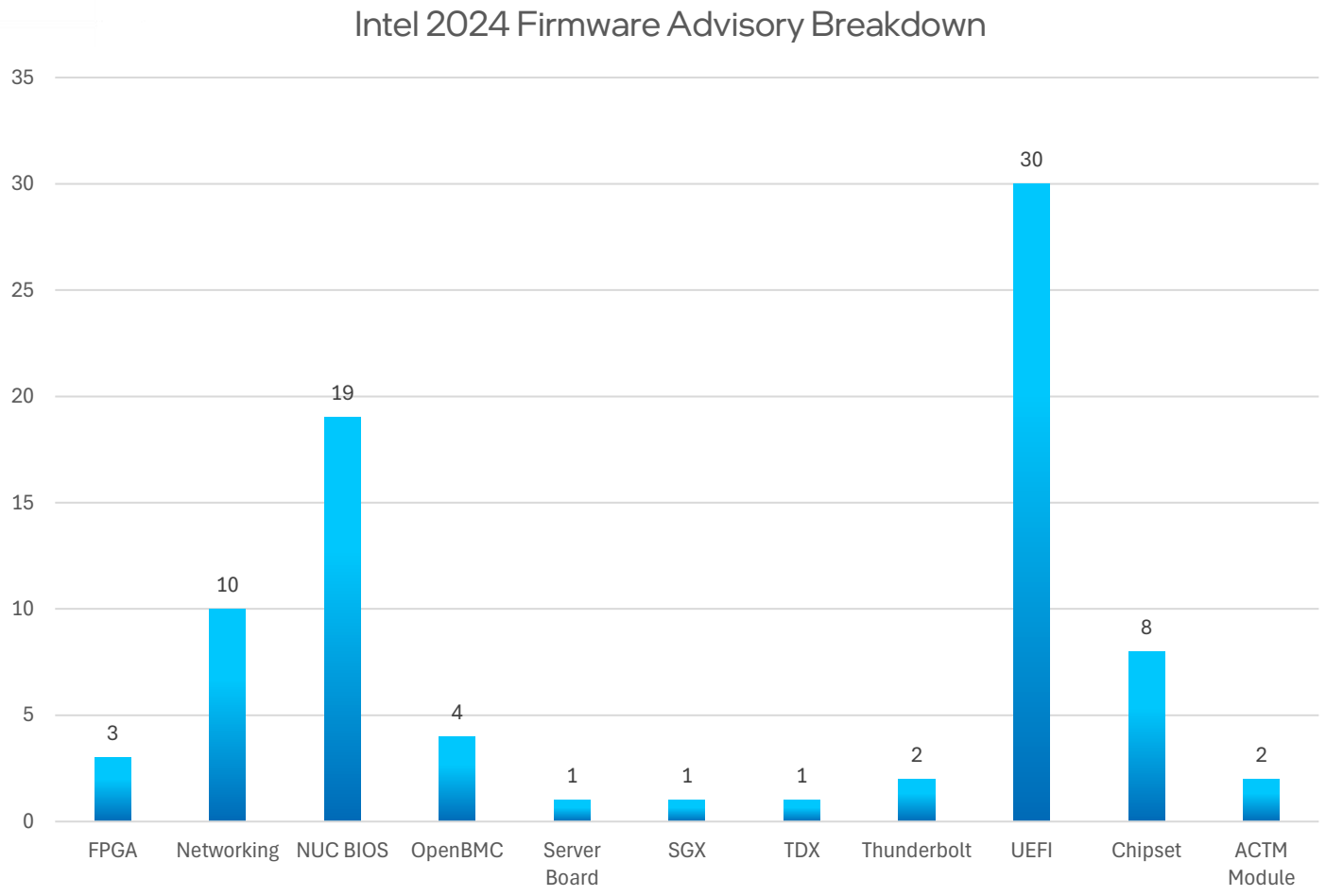
Further Breakdown of Intel Firmware Advisories

In 2024, Intel disclosed 81 CVEs in the firmware category. 97% of these issues were discovered as a result of Intel's proactive product security assurance efforts.

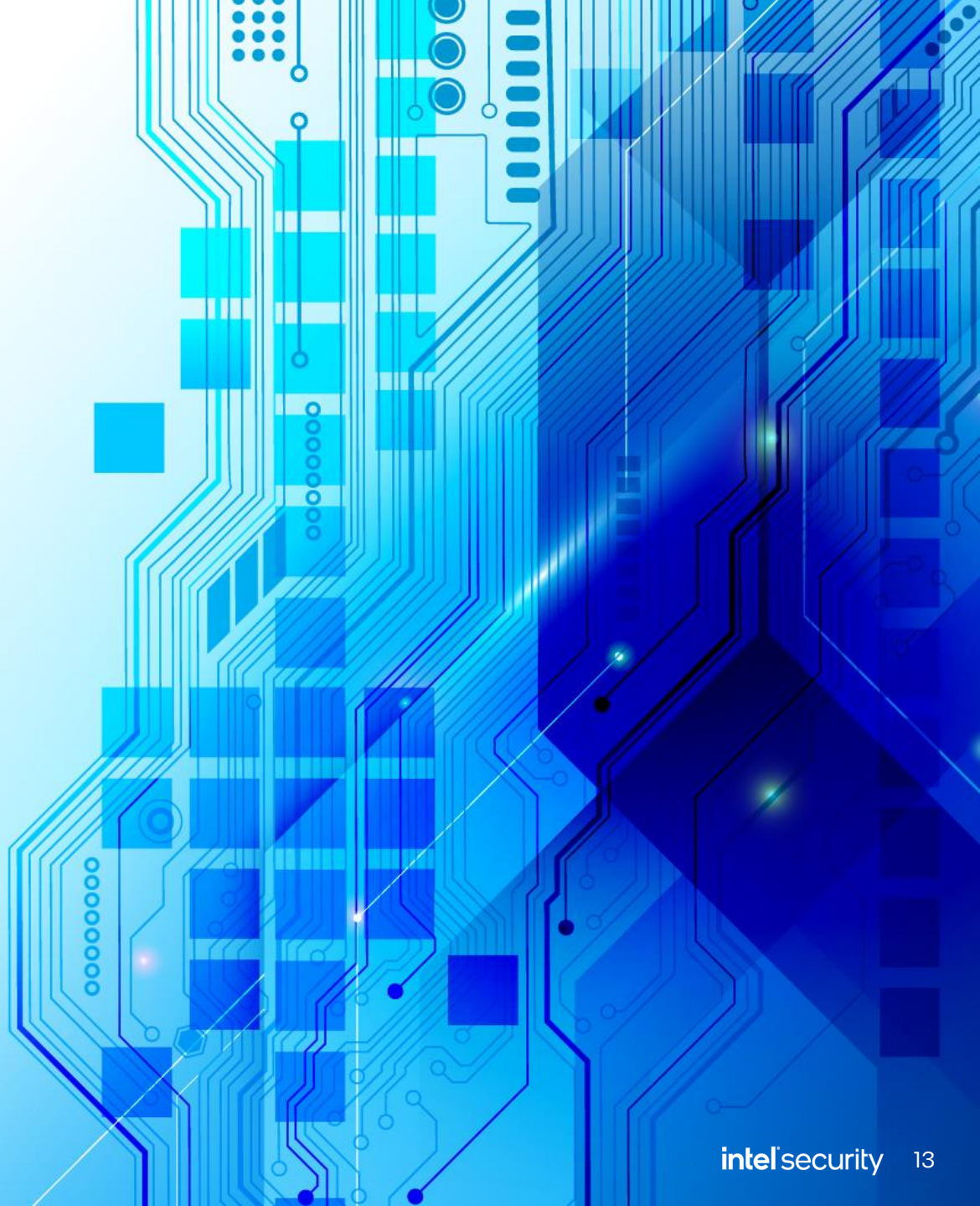
Further breakdown of the top 4 product areas:

- **Networking:** Firmware updates for found in Intel® Ethernet Controller I225 and Intel® PROSet/Wireless WiFi and Bluetooth® were all found internally by Intel researchers.
- **NUC BIOS:** As of January 16, 2024, support services for Intel® NUC products transitioned to ASUS. 13 of these CVEs were issued by a third-party BIOS vendor.
- **UEFI:** 14 of these issues were discovered in Intel® Server Products with the remaining issues affecting a mix of Client and Data Center platforms.
- **Chipset:** All 8 CVEs were found internally by Intel researchers.

Firmware updates are generally available through systems manufacturers (click for a list of support sites).



Platform Firmware Competitive Vulnerability Analysis

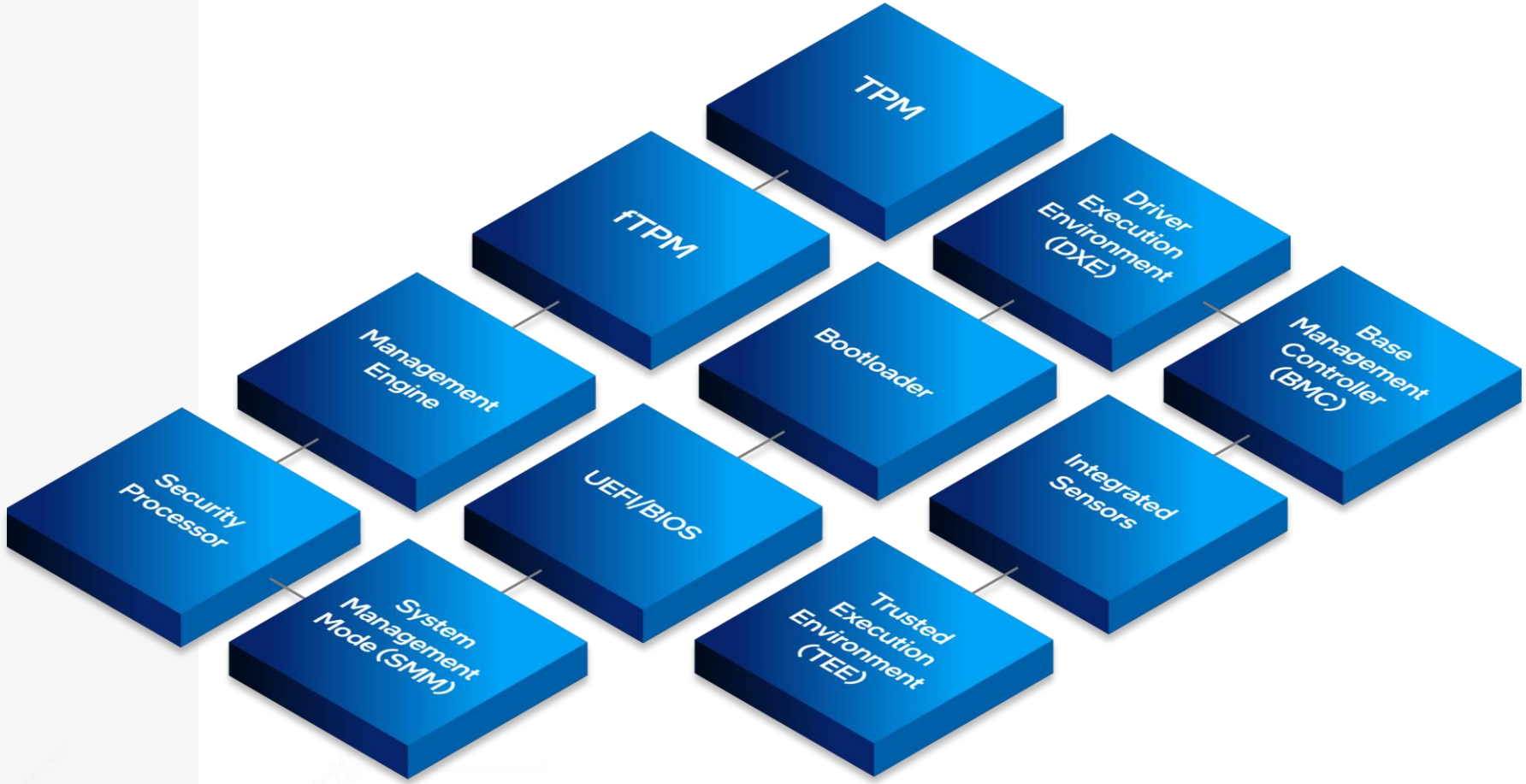


Platform Firmware

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 represents platform firmware.

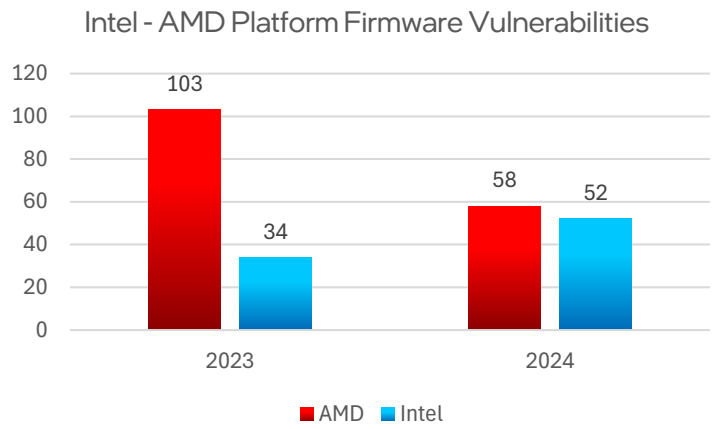
These examples also represent some the types of firmware where vulnerabilities were disclosed in either Intel or AMD products.

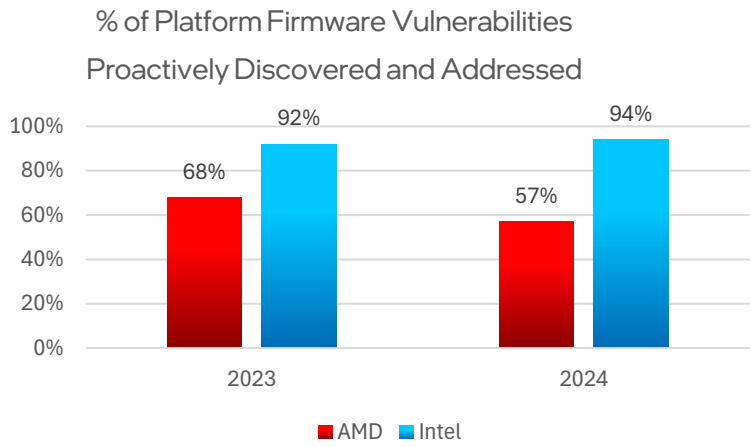


Platform Firmware Vulnerabilities

Key data points:

- In 2024, Intel reported 52 platform firmware vulnerabilities, while AMD reported 58.
- Intel's proactive product security assurance efforts resulted in the discovery and mitigation of 94% of platform firmware vulnerabilities.
- According to AMDs public security bulletins, they proactively discovered 57% of the platform firmware vulnerabilities disclosed in 2024.





Intel continues to raise the bar with the proactive discovery and mitigation of 94% of its platform firmware vulnerabilities in 2024.

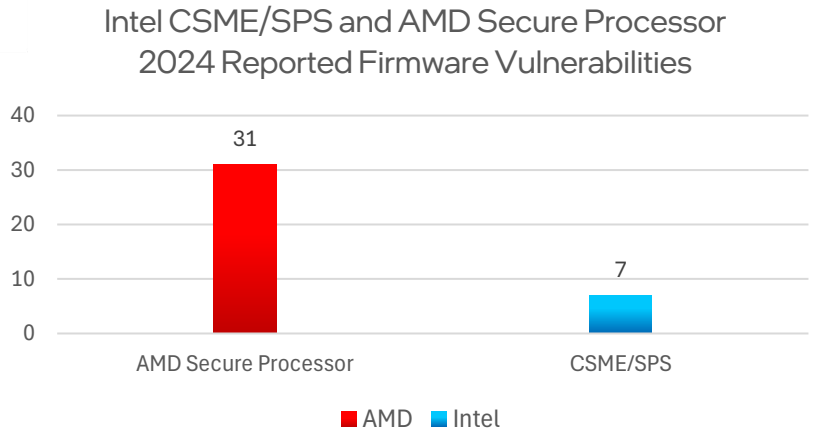
Hardware Root-of-Trust

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

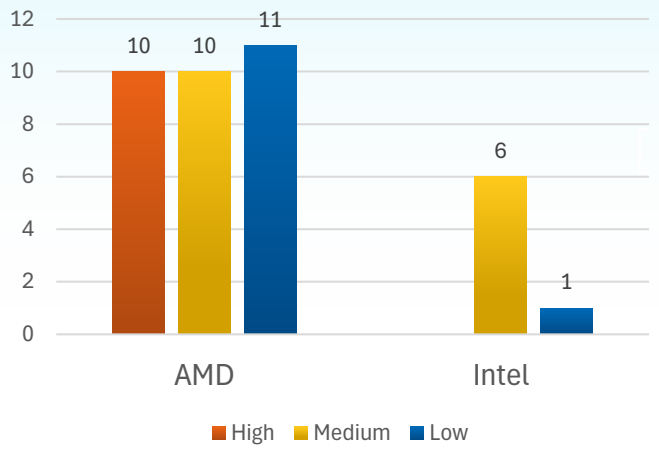
AMD ASP is also responsible for other security operations, such as memory encryption for confidential computing, whereas Intel platforms rely on other features, such as MCHECK, which has had no discovered vulnerabilities in recent years.

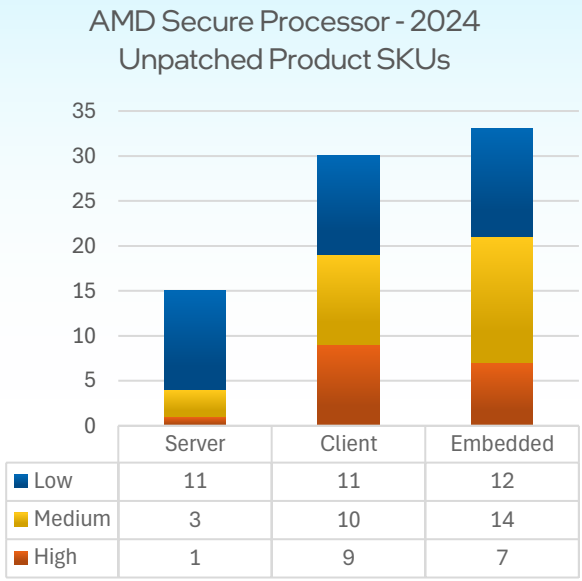
Key data points:

- AMD reported ten high-severity vulnerabilities in the AMD Secure Processor.
- In 78 instances, supported product SKUs affected by AMD Secure Processor vulnerabilities were listed as "No fix planned".
- Intel provided mitigations for all supported product SKUs affected by vulnerabilities in its hardware root-of-trust firmware.
- Five of the high-severity vulnerabilities reported in AMD's Secure Processor could allow an attacker to achieve arbitrary code execution.
- 100% of the Intel vulnerabilities in the Root-of-Trust category were found internally by Intel employees.
- 42% of the AMD vulnerabilities in the Root-of-Trust category were found by external security researchers.
- AMD's confidential computing technology, SEV-SNP, was compromised through vulnerabilities in the AMD Secure Processor*.



In 2024, AMD reported 4.4x more firmware vulnerabilities in their hardware root-of-trust than Intel.





	Server	Client	Embedded
Low	11	11	12
Medium	3	10	14
High	1	9	7

* https://www.blackhat.com/us-24/briefings/schedule/index.html#all-your-secrets-belong-to-us-leveraging-firmware-bugs-to-break-tees-40137

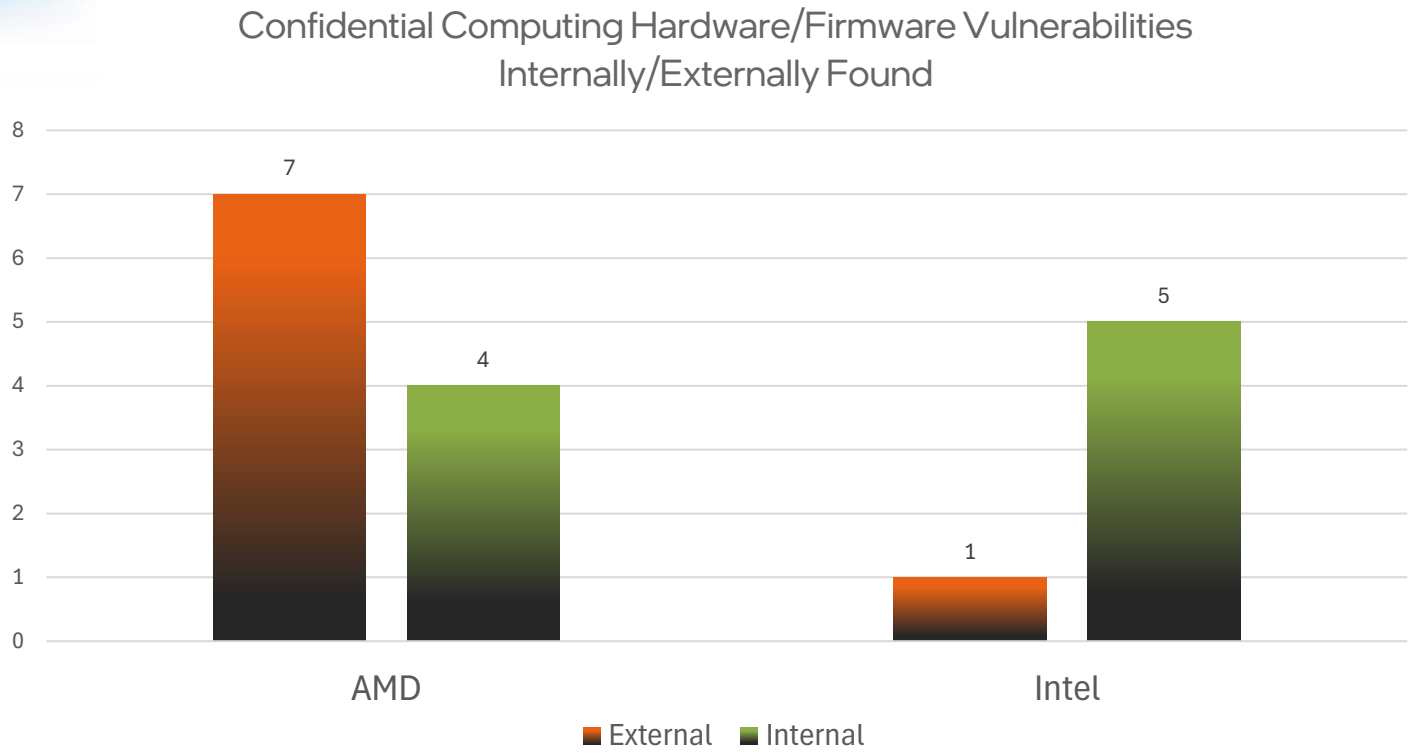
Confidential Computing Firmware

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).

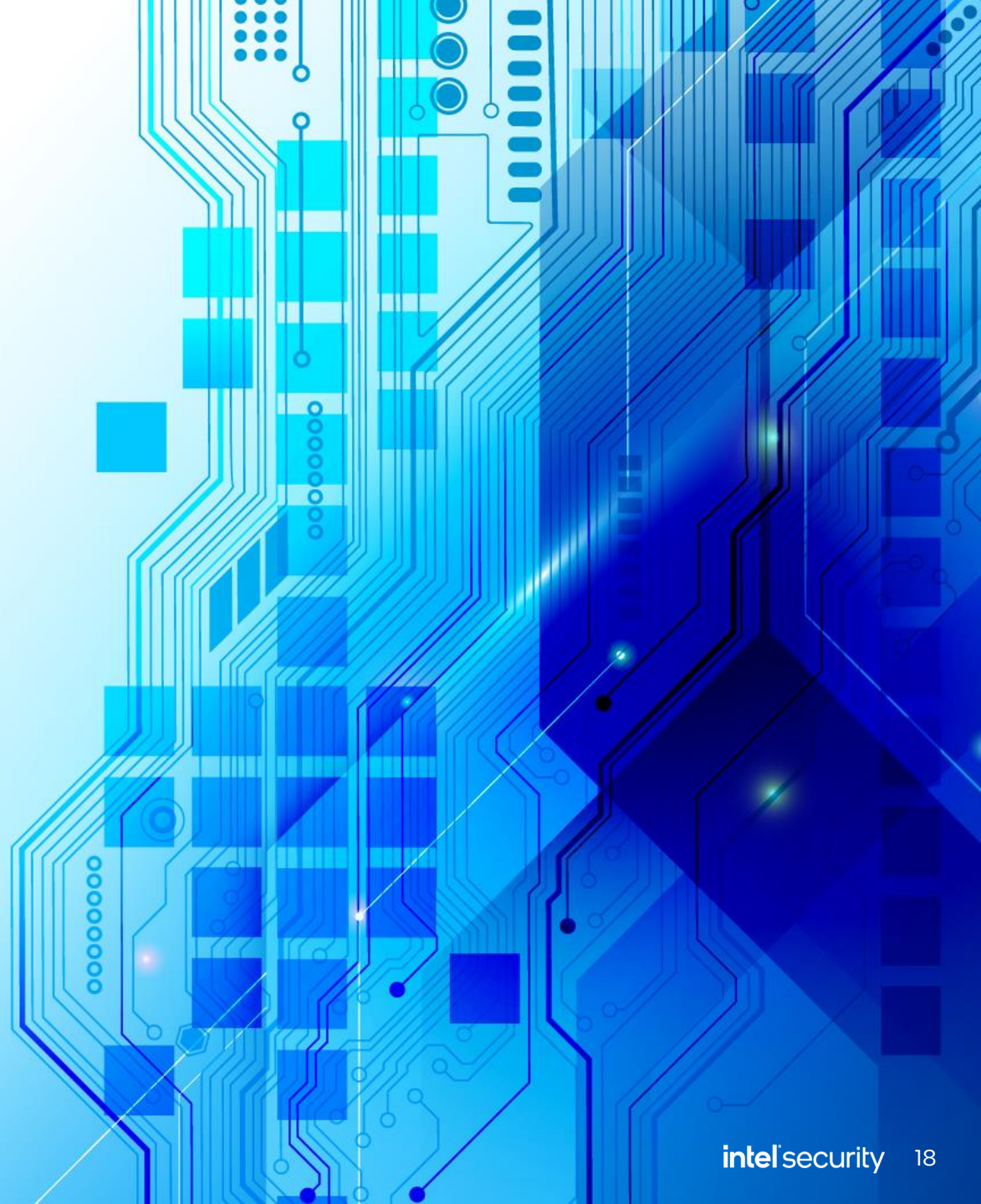
AMD: Secure Encrypted Virtualization (SEV), SEV-ES (Encrypted State), and SEV-SNP (Secure Nested Pages).



In 2024, AMD reported 1.8x more vulnerabilities in their Confidential Computing firmware components and features than Intel.

Intel found 83% of Confidential Computing firmware vulnerabilities internally in 2024, while AMD found 36%.

Graphics Processing Unit (GPU) Competitive Vulnerability Analysis

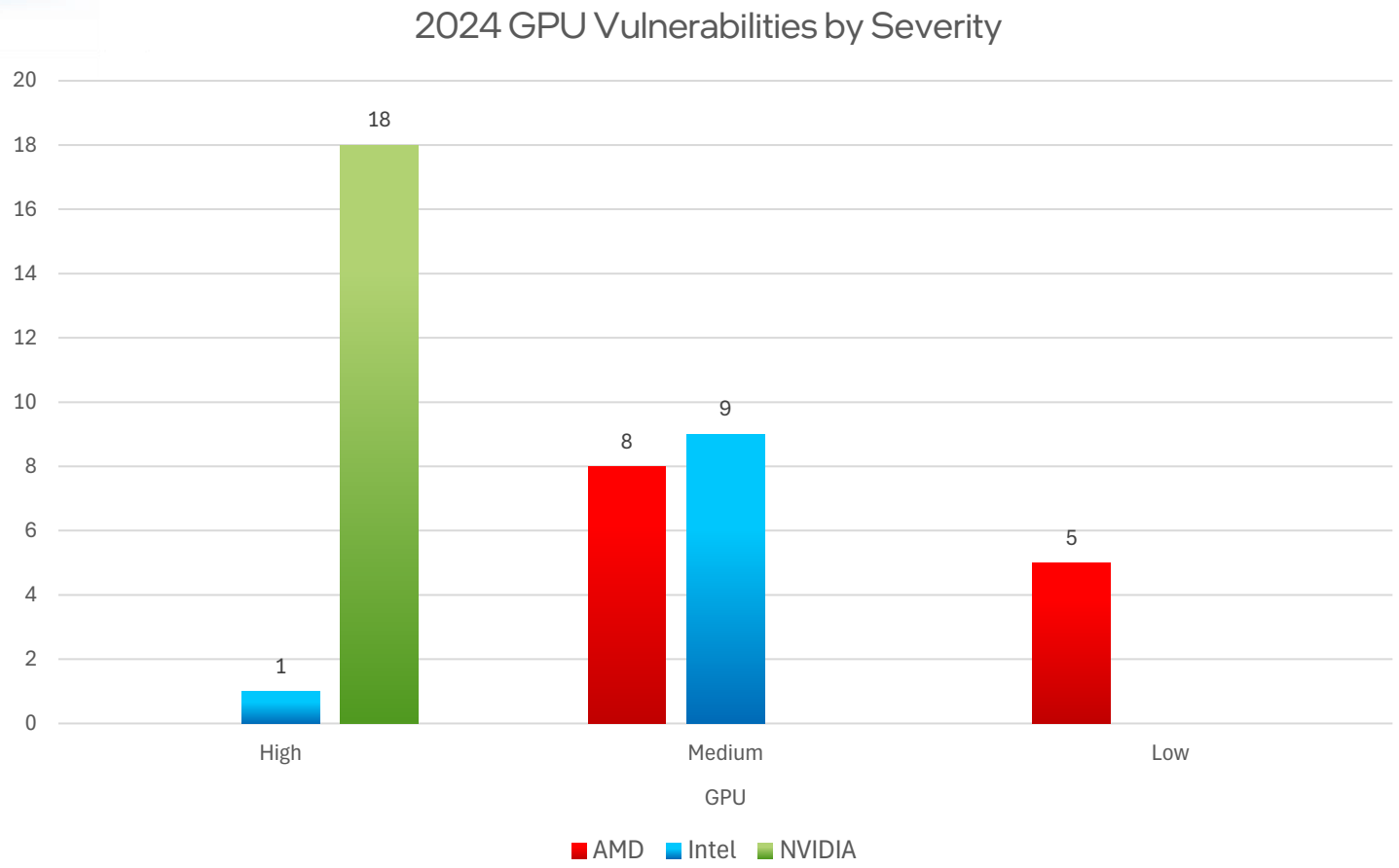


2024 GPU Vulnerabilities by Severity

The graphics processing unit, or GPU, has become one of the most important types of computing technology, both for personal and business computing. Designed for parallel processing, the GPU is used in a wide range of applications, including graphics and video rendering. Although they're best known for their capabilities in gaming, GPUs are becoming more popular for use in creative production and artificial intelligence (AI).

Key data points:

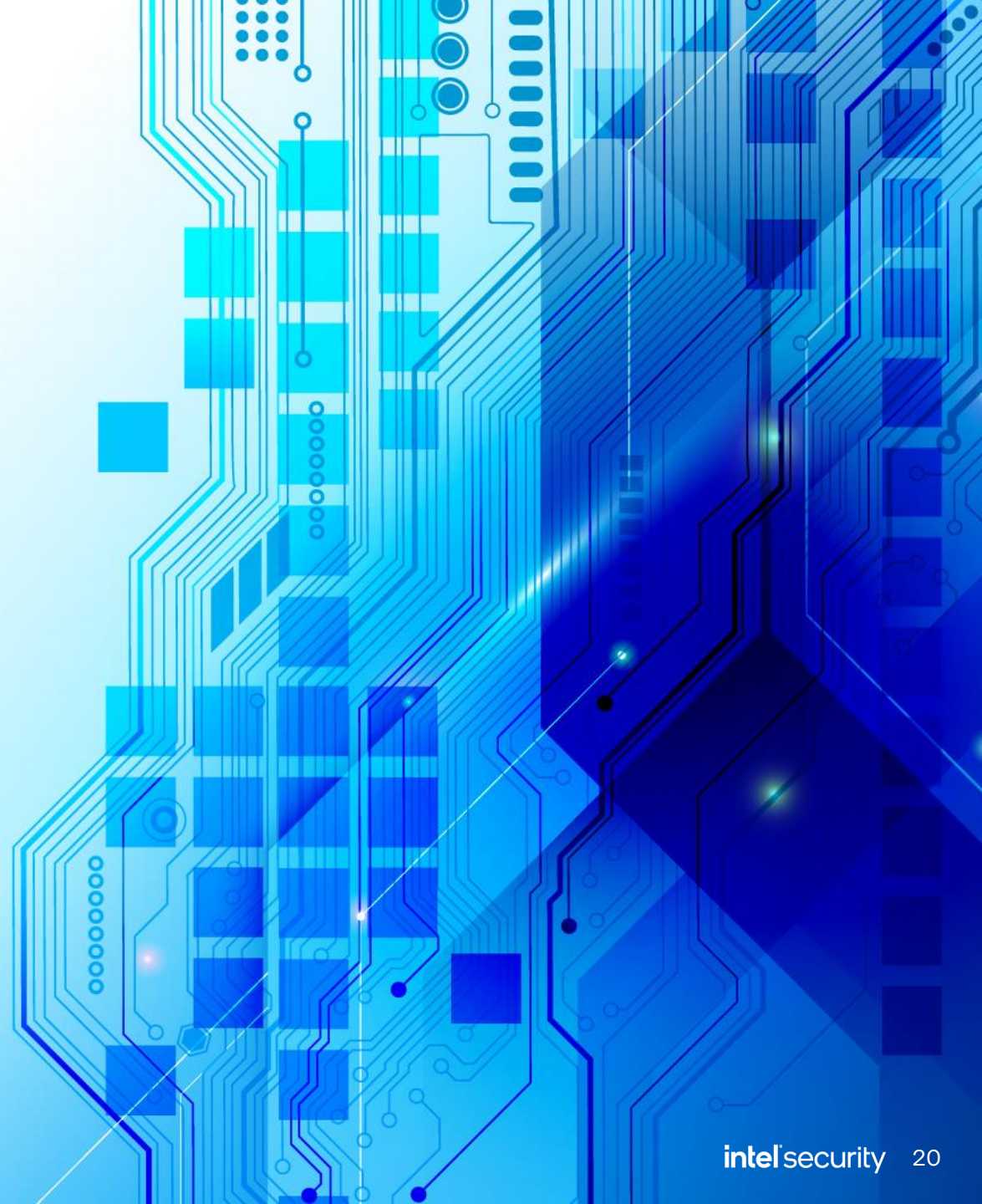
- Intel had the fewest number of GPU vulnerabilities in 2024 at 10, while AMD had 13 and NVIDIA posted 18.
- In 2024, 100% of NVIDIA's GPU-related vulnerabilities were high severity.
- In 2024, 72% of NVIDIA GPU-related vulnerabilities had the potential to allow an attacker to execute code of their choice.



100% of NVIDIA GPU-related vulnerabilities were HIGH severity, with 72% potentially resulting in code execution.

Platform Servicing

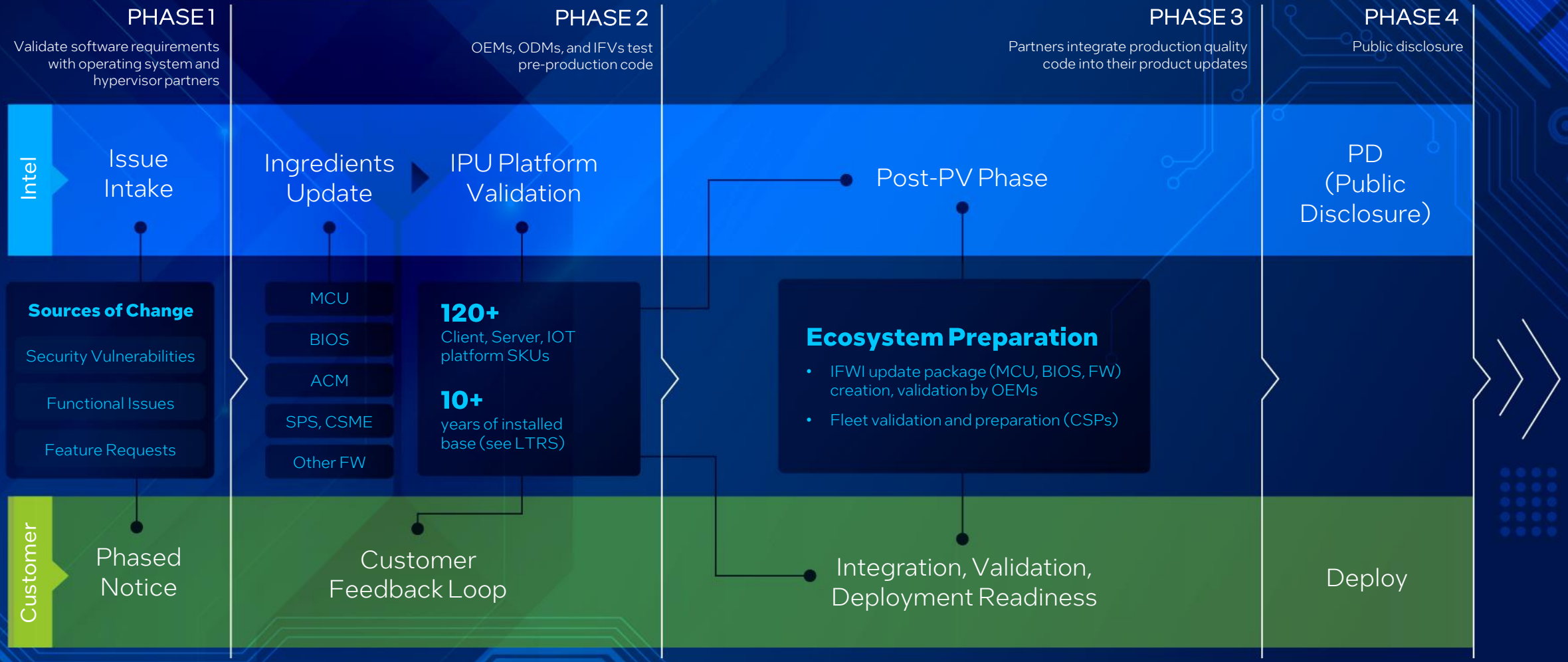
An in-depth look at the industry-leading process of updating platform firmware and microcode across a global network of partners and customers.



Intel Platform Update (IPU) Process

Quarterly process consisting of security, functional, and feature updates in microcode, firmware, and system BIOS

The IPU enables Intel partners to validate and integrate hardware and firmware updates into their platforms on a predictable quarterly schedule, leading to coordinated public disclosure across the ecosystem.



Intel Long-Term Retention and Support (LTRS): A Product Assurance Game Changer

A unique capability positioning Intel as an industry leader for supporting our customers with long-term product assurance

Long-Term Retention and Support (LTRS) is a unique investment in the silicon industry and a key factor in ABI Research naming Intel #1 for product security assurance. LTRS is integrated into the product development process across three critical phases:

1. **Tape Out (TO)** is when a new design is handed off to manufacturing. Collaterals collected at this phase include High-Level Architectural Specifications, IP reference releases, SOC, and code modules. All collaterals are tagged and stored for the life of the product and beyond.

2. **Production Release Qualification (PRQ)** occurs when the first silicon parts are produced. Here, additional documentation is collected, as well as component debug information and Processor Platform Validation (PPV) materials, including test plans and hardware, firmware, and software collaterals.

3. At the **Production Validation (PV)** phase, the silicon is now approved for mass production. All related binaries, software and firmware ingredients, architecture specifications, bill of materials, and test/debug collaterals are collected in addition to actual hardware.

LTRS supports ongoing debugging needs and the Intel Platform Update process. It is available 24x7 with dedicated on-site support. Intel engineers can have nearly any platform configured and ready for testing and validation work within minutes.

Long-Term Retention and Support (LTRS) enables a competitive advantage for Intel and a unique value for our customers

SW Doc

Tape Out (TO)

(Design hand-off to the fab)

Over 20 petabytes of Integrated Circuit collaterals archived

SW Doc HW

Production Release Qualification (PRQ)

1000's of SW, Docs, and HW saved in a centralized location, easily/remotely accessible

HW SW BOM SW Doc

Production Validation (PV)

Everything an engineer needs, accessible within minutes

Long-Term Retention & Support

- Drive cross-Intel policies, execution, and governance for the retention of necessary product collaterals required for long-term assurance
- LTRS Costa Rica Hub operates as a world-class cross-Intel lab for engineering support of critical product servicing needs

4500+

Platforms online with 24x7 access and support

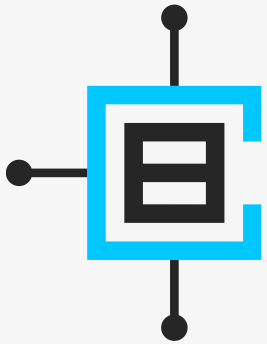
Bug Bounty Program

Intel Bug Bounty Program

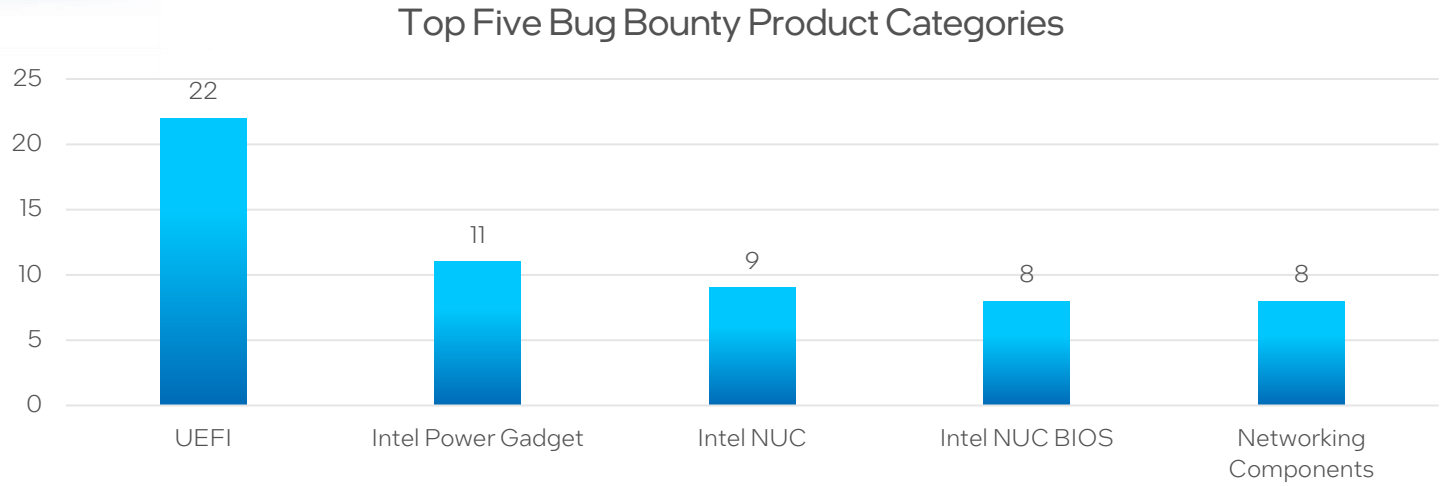
Intel's Bug Bounty program is a key component of Intel's silicon industry leading product security assurance. It provides incentives to external security researchers to find, report, and coordinate the disclosure of vulnerabilities when mitigations are available for customers.

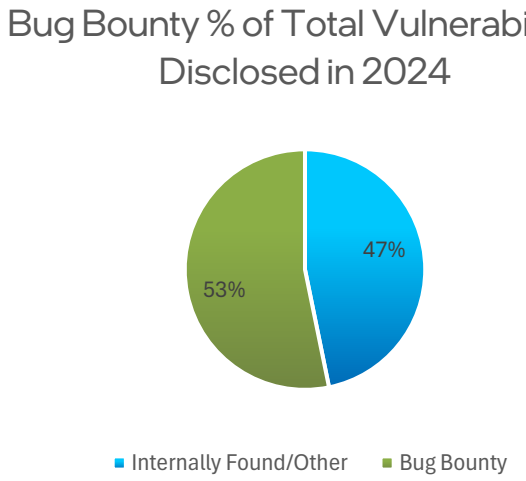
Key data points:

- Intel's Bug Bounty program accounted for 53% of the vulnerabilities addressed in 2024.
- 84% of bounties paid in 2024 were for software issues and 16% were for firmware.



[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.





Intel's deep engagement with the security research community drives the success of its Bug Bounty program resulting in 53% of the vulnerabilities addressed in 2024.

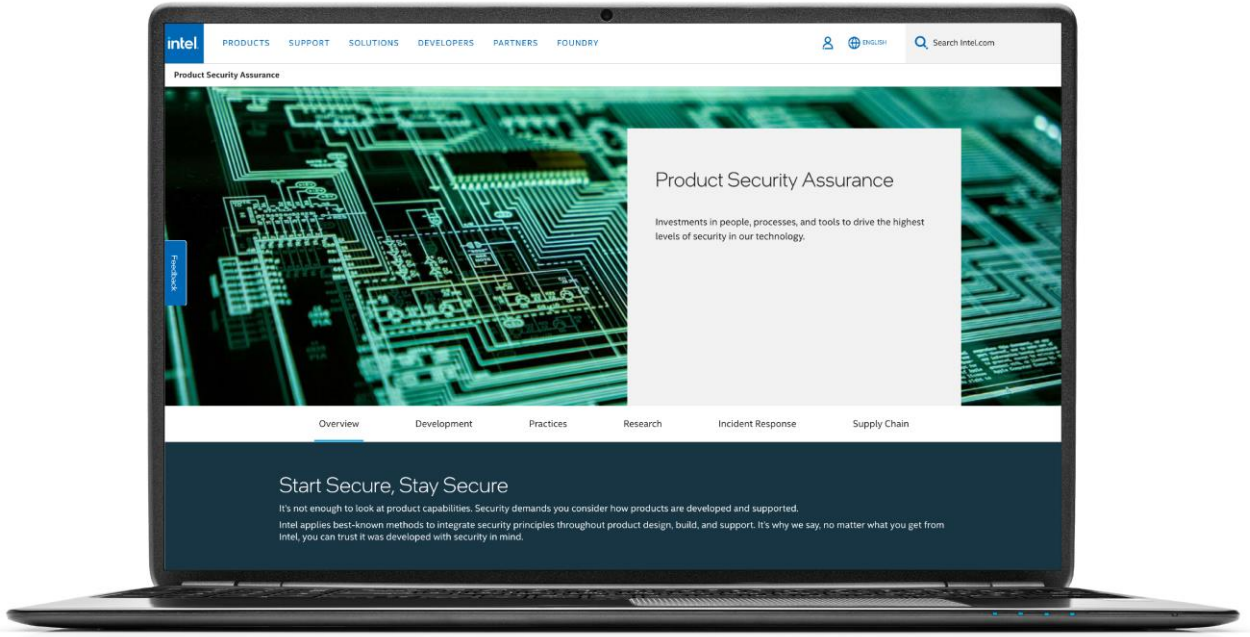
Reference

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.



Resources and References

Intel Security Advisories

AMD Security Bulletins

NVIDIA Security Bulletins

ABI Research Report on Product Security Assurance

IBM, Cost of a Data Breach Report 2024

Systems Manufacturer Support Sites

Product Security Assurance at Intel

Intel's Security First Pledge

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.