2021 Product Security Report

intel security

“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 security

Contents

2021
Key Stats

intel security

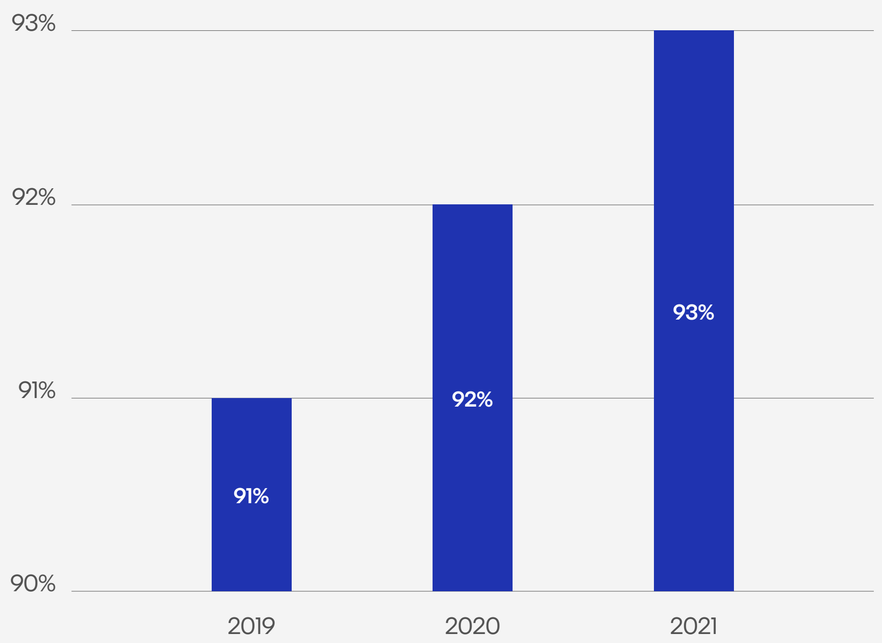
93% (up from 92% in 2020) of vulnerabilities addressed are the direct result of Intel's investment in product security assurance. Intel's proactive efforts continue to drive this percentage up year over year.

50% of the 226 CVEs published were discovered internally by Intel employees.

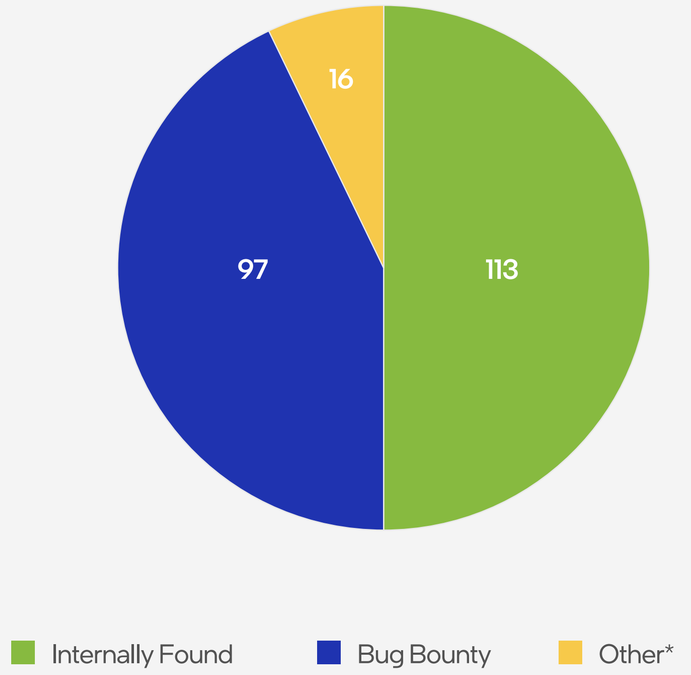
86% of the 113 vulnerabilities reported by external researchers, 97 (86%) were reported through Intel's Bug Bounty Program.

77% (up from 69% in 2020) of hardware/firmware vulnerabilities were found by Intel while 70% (down from 83% in 2020) of software issues were found by external researchers.

% of vulnerabilities found through proactive efforts



Intel's investment accounts for 93% of vulnerabilities addressed in 2021



* Other consists of reports through open source projects managed by Intel and from organizations who do not or cannot seek bug bounty payments.

Foreword

Securing hardware is the foundation to all security efforts.

Attackers are increasingly targeting hardware, as attacks at the hardware level can enable greater control to the attacker over software exploitation. Secure hardware provides a trusted foundation to protect data and empowers software to provide greater protection and functionality with a basis in hardware.

At Intel, security comes first both in the way we work and in what we work on. Our culture and practices guide everything we build with the goal of delivering the highest performance and optimal protections. We are relentless in our pursuit of innovation, taking a security-centric approach that enables our customers to tackle today's toughest challenges.

As with previous reports, the 2021 Intel Product Security Report demonstrates our Security First Pledge and our endless efforts to proactively seek out and mitigate security issues.

In 2021 we delivered mitigations for 226 product security issues. Of the 226 issues addressed, 113 (50%) were found internally by Intel employees and another 97 (43%) were reported through Intel's Bug Bounty program. In total, 93% of the vulnerabilities addressed were the result of Intel's proactive efforts in product security assurance.

We design with security in mind.


Security
@ Intel
intel security

“As cybersecurity threats advance and attack surfaces increase, Intel is helping customers respond to attack vectors and keep their systems and data better protected by building layers of defense using our hardware, software and security assurance expertise. We’re driving to innovate beyond what we once thought possible.”

Greg Lavender
Chief Technology Officer

intel security

At Intel, security comes first.

In the way we work:

Practices

Our culture and practices guide everything we build with the goal of delivering the highest performance and optimal protections

- Secure Development Practices
- Threat Discovery & Response
- Community & Policy Advocacy

In what we work on:

Technology

We are relentless in our pursuit of innovations, taking a security-centric approach, that enables our customers to tackle today's toughest challenges

- Software Reliability
- Workload Protection
- Foundational Security

Download the Security @ Intel document here and watch the Chips & Salsa video discussion here.

Intel's Security First Pledge: Strengthening Our Commitment

System trust is rooted in security - if hardware isn't secure, then a system cannot be secure. At Intel, our goal is to build the most secure hardware on the planet, from world-class CPUs to XPUs and related technology, enabled by software. And we have sophisticated systems to find and address security vulnerabilities in our products.

Intel's commitment to security has never been stronger. We invest in unparalleled people, processes, and products, integrating security in the ways we work and everything we work on. As we relentlessly pursue the best solutions to protect customer systems and data, you can be confident Intel is committed to:

- **Unwavering Customer Focus.** We put customer needs first in our security decisions. We listen to their challenges and use this feedback to guide everything we research, architect, build, and release. Trust is rooted in transparency. We communicate security advisories and product updates to help customers stay informed and keep their systems protected.
- **Continuous Technology Innovation.** New threats will emerge and vulnerabilities will be found, so Intel is committed to growing, adapting, and relentlessly advancing security. From accelerating cryptography and Confidential Computing, to safeguarding our supply chain and manufacturing operations, we never stop innovating.
- **Robust Incident Response.** We invest extensively in vulnerability management and offensive security research for the continuous improvement of our products. The Intel Bug Bounty program is a critical way we incorporate outside perspectives, collaborating with researchers and leading academic institutions to find and address vulnerabilities. Intel role models best practices for incident response; when an issue is identified, we follow coordinated vulnerability disclosure practices to release findings and mitigations together.
- **Security by Design.** We follow rigorous policies and procedures spelled out in our Security Development Lifecycle (SDL) to integrate security principles and privacy tenets at every step of hardware and software development. Intel has dedicated experts driving a security-first mindset that starts with research and design and doesn't stop until products reach end of servicing.
- **Community Advocacy.** It's clear no single entity can solve complex security challenges alone. We work with technology partners, academic institutions, industry organizations, and governance bodies worldwide. These efforts support development of policies, industry guidelines, standards, and research to elevate shared security goals that benefit everyone.

We actively work to deliver security without sacrificing performance. Working with our customers and industry partners, we can achieve the levels of secure performance people expect and deliver technology they trust.

Investing in Security Assurance

intel security

“Security is not a feature, it is a mindset, and at Intel, a security first mindset is critical. It means continuously improving and raising the standards in both what we work on and how we work on it. It is the intentional design of our products to include the latest security updates along with layers of new capabilities that aim to address entire classes of attack. This combination of technology capabilities, secure design and a security mindset comprehensively helps our customers solve their most difficult challenges.”

Mohsen Fazlian

Corporate Vice President and General Manager,
Intel Product Assurance and Security

intel security

Security Development Lifecycle (SDL)

The Intel Security Development Lifecycle (SDL) guides us in applying privacy and security practices across hardware and software (including firmware) throughout the product lifecycle.

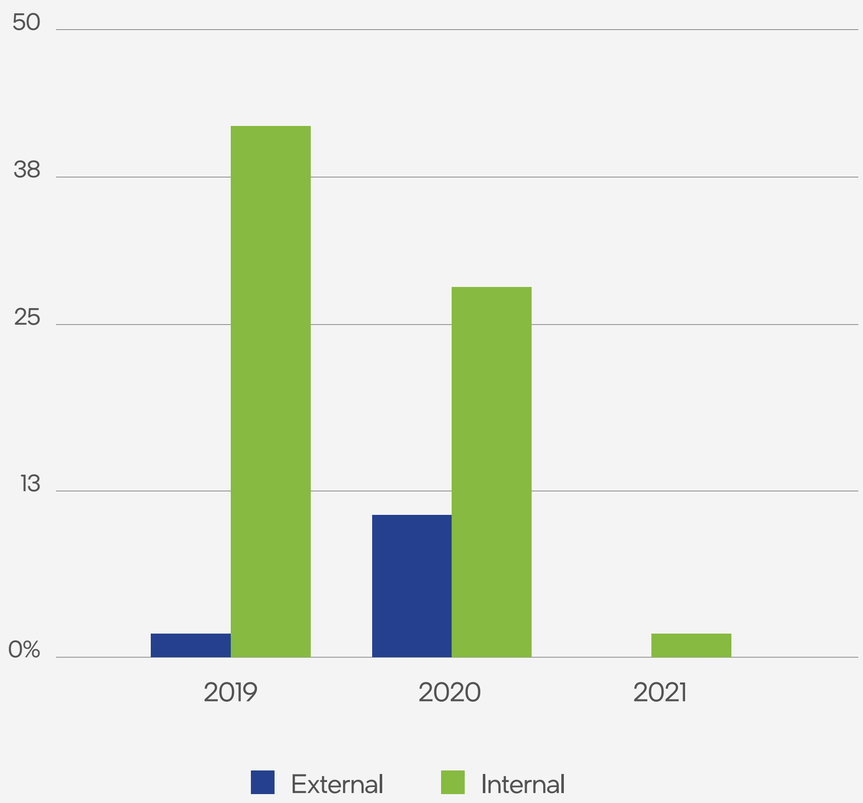
More information about Intel's SDL program.

SDL Spotlight – Intel® CSME

Intel has made a significant investment in Intel Converged Security and Management Engine (CSME) Security. Security Assurance practices across the SDL have been enhanced with automated detection tools as well as over a dozen hackathon events, code reviews by internal security experts, advanced pen testing, contracted reviews by external security firms, and ongoing collaboration with the external researcher community.

To help ensure the robustness of CSME security, 40 design changes from ME13 through ME16 were implemented, including Data Protection, Control Flow protection, and CET HW in the CSME microcontroller starting with Tiger Lake platforms.

As a result of these efforts, there has been a steady decline in vulnerabilities discovered with a total of 6 medium severity issues found in 2021, all by Intel security researchers.



Bug Bounty Program

The community of security researchers from around the world continue to contribute to improving the security of technology in many ways. Collaboration on security research yields improved identification and mitigation of potential vulnerabilities and coordinated vulnerability disclosure allows all parties time to develop and deploy mitigations. We value these contributions and, through our Bug Bounty program, aim to reward researchers.

In 2021, we launched our Bug Bounty Bonus program across Intel Pentium®, Celeron® and Atom® Processors. This marked the first of several planned expansions to the program and began rewarding researchers with bonus multipliers for findings in specific areas of interest.

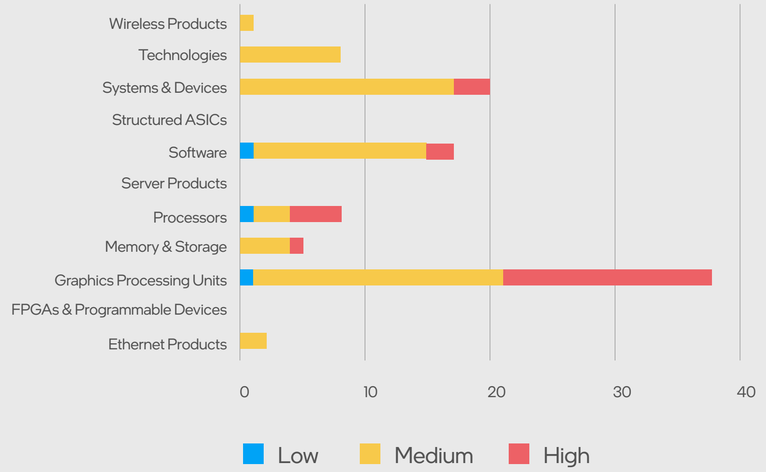
Across the entire Bug Bounty program, top areas of findings for researchers were in GPUs, system and devices, and software, leading to mitigations and improved security across an array of products.

As Intel works to continuously improve its security, we would like to acknowledge the incredible research being done across the community and the talent driving it. At right is the list of our top researchers for 2021 by payout. Thanks to all who have participated in our Bug Bounty programs!

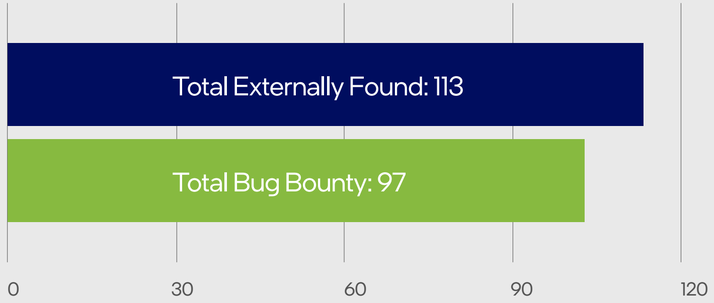
Intel's Top Researchers for 2021 (by payout)

1. Hugo Magalhaes
2. breaker
3. allowetotima
4. dreamercat
5. *anonymous
6. *anonymous
7. *anonymous
8. *anonymous
9. mmg
10. star-labs
11. *anonymous
12. *anonymous
13. avivanoa
14. *anonymous
15. *anonymous

* Indicates researcher chose to remain anonymous



86% of External Reports are from the Bug Bounty



Project Circuit Breaker
Intel's Bug Bounty

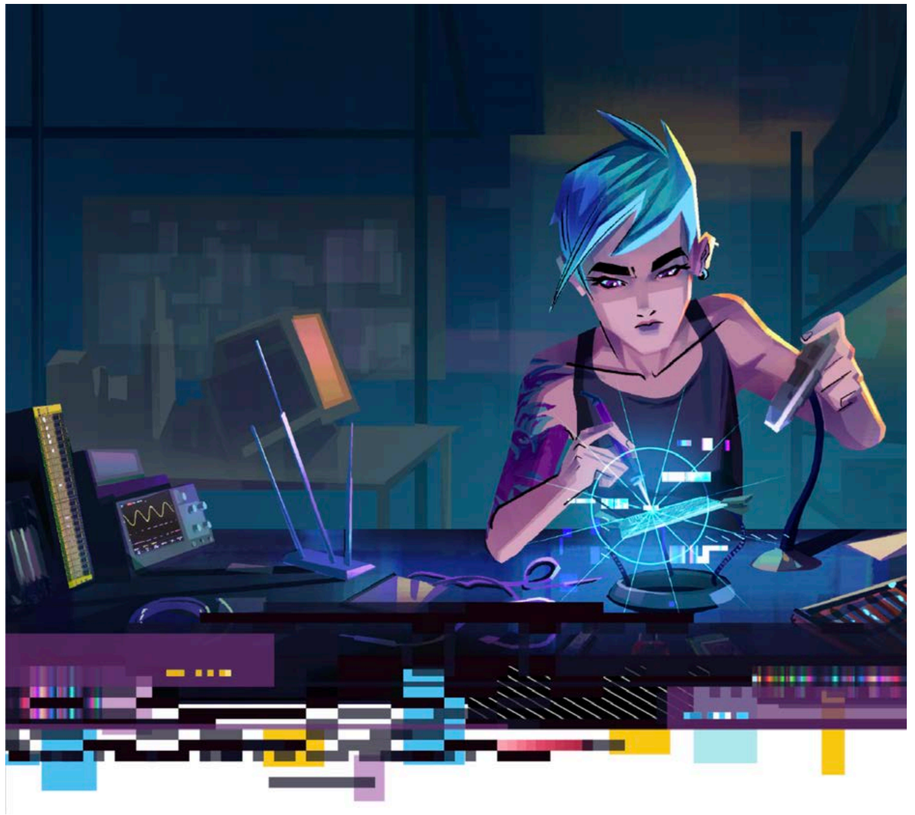
New for 2022, Intel invites security researchers to join Project Circuit Breaker, a community of elite hackers hunting bugs in firmware, hypervisors, GPUs, compromising chipsets, pwning processors and much more.

In this next expansion of Intel's Bug Bounty program, we're creating a community dedicated to offering training to security researchers, exciting new hacking challenges and opportunities to work at unprecedented levels with new and pre-release products, as well as new collaborations with Intel hardware and software engineers.

For the first time, we're creating opportunities to be invited to and/or apply for special security research events. These live, timeboxed events will focus efforts on new technologies where we see the community having a greater security impact. As the new normal sets in, one where the real world and the digital world are becoming the same, we're working to address increased attack surfaces and threats through the power of community.

All of this is driven by our commitment to work in the open, be transparent and demystify the experience for security researchers. We seek to remove the barriers to entry that, in the past, have left potential expertise untapped.

A new day, a new circuit to break. Join the movement at projectcircuitbreaker.com.



Industry Initiatives

As with any broad technological hurdle, security challenges cannot be fully addressed by a single institution acting alone. That's why Intel initiates and leads the industry in wide ranging efforts to advance capabilities and infrastructure crucial to the security assurance of hardware/software technologies and products.

Our Security First Pledge means that we work to enhance the security of the entire ecosystem, benefiting not just our customers, but also competitors. We engage in cross-industry collaboration that aids in the development of future security technologies and the creation of innovative security mitigations. We know that our products, whether in the data center, on the edge, or on the desktop, are built on a foundation of trust.

Industry collaboration is a key and strategic component to how we seek to lead in hardware security innovation. Every day we collaborate with the leading operating system, hypervisor, and cloud services providers, to work on microarchitectural solutions that have impact on a global scale. It is truly amazing when companies, some of which may be competitors in the global market place, can work together on solutions that benefit the entire ecosystem.

Technology Standards

Intel leads and participates in industry consortiums and standard bodies shaping how technologies should be designed to meet security, privacy and safety requirements. This includes feature and mitigation requirements aligned to anticipated use cases as well as emerging threat landscape generated by our security research. Examples include:

- Trusted Computing Group (TCG)
- Confidential Computing Consortium (CCC)
- 3rd Generation Partnership Project (3GPP)
- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)

General Product Design, Assurance & Risk Management Standards

As vulnerability research methods become more sophisticated, often targeting hardware, Intel is driving secure-by-design best practices, systemic mitigations, automated vulnerability scanning tools, and hardware security training, among other efforts.

- MITRE: Intel collaborated to extend existing community-driven software-oriented Common Weakness Enumeration (CWE) to include 98 hardware weaknesses and is involved in Common Vulnerabilities and Exposures (CVE) and Common Attack Pattern Enumeration and Classification (CAPEC).
- Forum of Incident Response and Security Teams (FIRST): Intel participates in the Common Vulnerability Scoring System (CVSS) and Product Security and Incidence Response (PSIRT) special interest groups (SIG).

Chips & Salsa Video: Intel's contribution to debug technology standards.

Industry Spotlight: Hardware CWEs

Intel helped drive the creation of the community-driven Hardware Weakness Enumeration (CWE) that resulted in the 2021 CWE most important hardware weaknesses list (details can be found here) as well as 98 total hardware weakness patterns in 12 categories.

The goal of the list is to drive awareness of common hardware weaknesses through CWE, and to help prevent hardware security issues at the source by educating designers and programmers on how to eliminate these issues early in the product development cycle.

Why is this important? According to Intel's Jason Fung, who helped to launch this effort with MITRE in 2019, "by using hardware CWEs, we can direct attention to specific areas to investigate for systemic mitigations, education, tooling, and ultimately, lift the industry to a higher level of security."

2021 CWE Most Important Weaknesses

CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

Chips & Salsa Video: Learn more about the importance of hardware CWEs from Jason Fung.

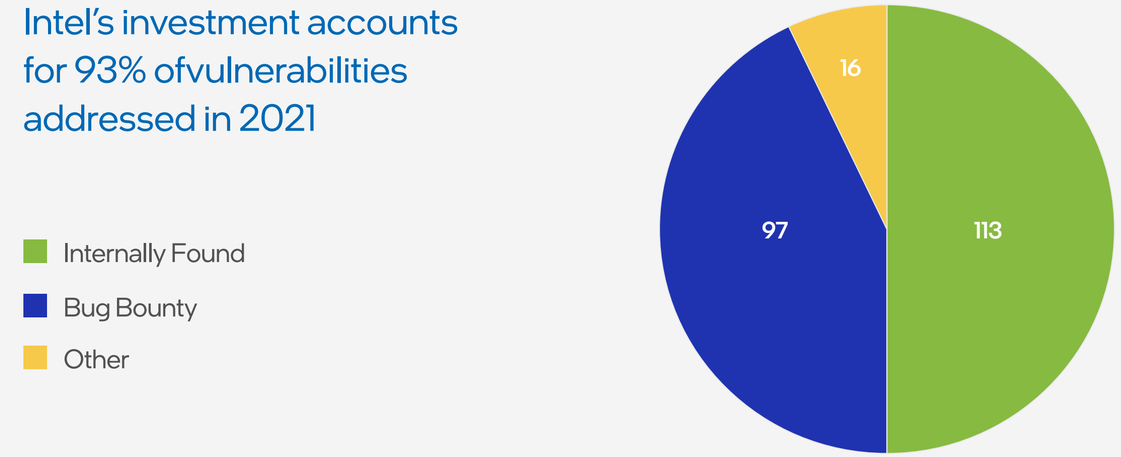
Results of Intel's Investments in Security Assurance

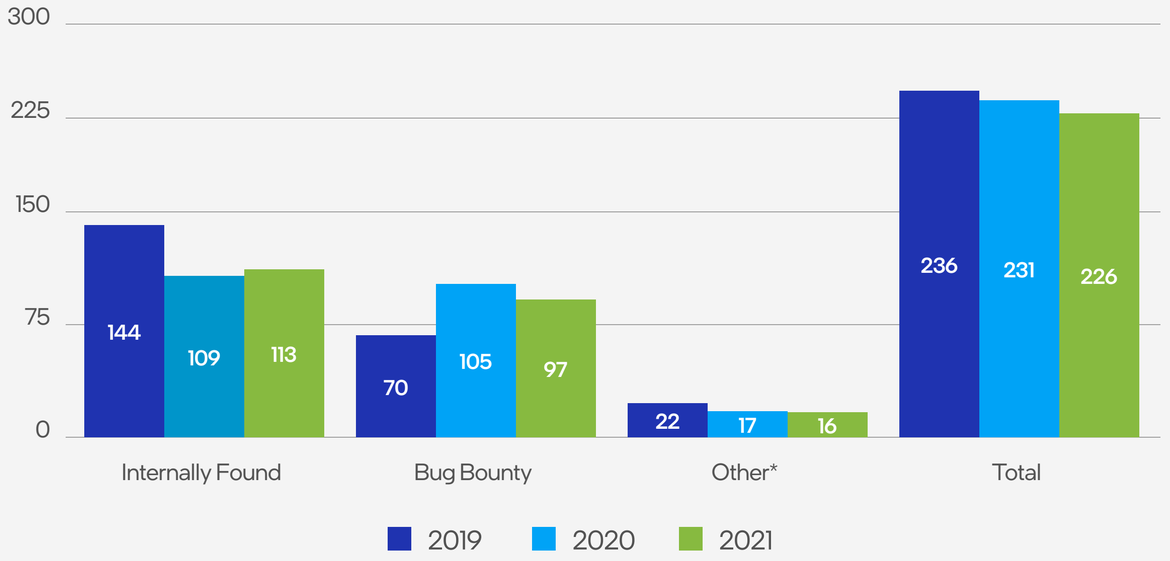
Since the first product security report covering calendar year 2019, Intel continues to raise the bar on proactively finding and mitigating product security issues in an effort to help ensure our products form the root of trust for protecting customer data. This is accomplished through a robust SDL program, internal red team events and a mature vulnerability management program.

Internal security research for 2021 accounts for 50% of the issues addressed and an additional 43% were reported through Intel's Bug Bounty Program.

In 2021, we addressed 226 vulnerabilities compared to 231 in 2020 and 236 in 2019.

Intel's investment accounts for 93% ofvulnerabilities addressed in 2021





* Other consists of reports through open source projects managed by Intel and from organizations who do not or cannot seek bug bounty payments.


2021 CVE Data
intel security

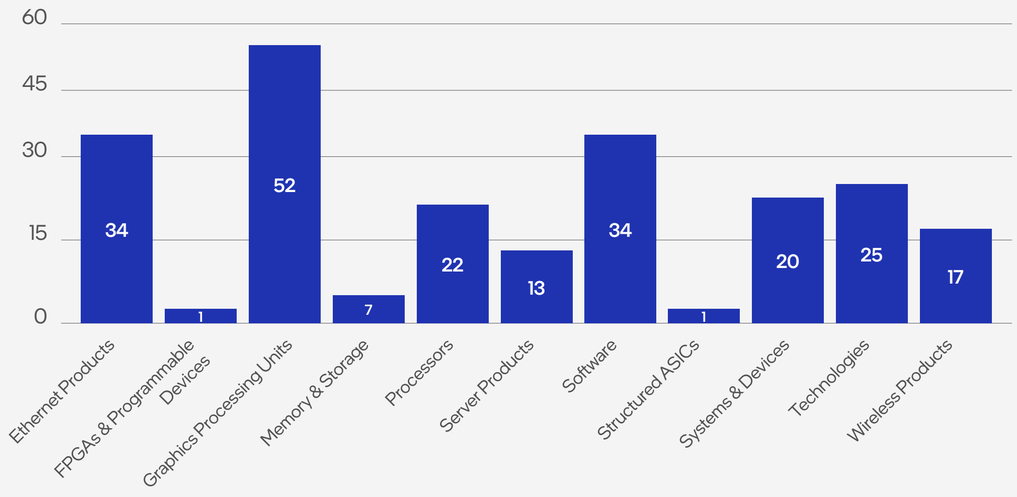
CVE DATA

CVEs by Category

Intel has a vast product portfolio and this report breaks out vulnerability information into product categories as seen on www.intel.com.

Intel's proactive product security assurance efforts resulted in 93% of the vulnerabilities published in 2021. On the pages following, CVE data is broken out by internally and externally found and by severity according to the Common Vulnerability Scoring System (CVSS).

CVE Count by Product Category – 2021



For more information on Intel product categories, see reference section.

CVE DATA

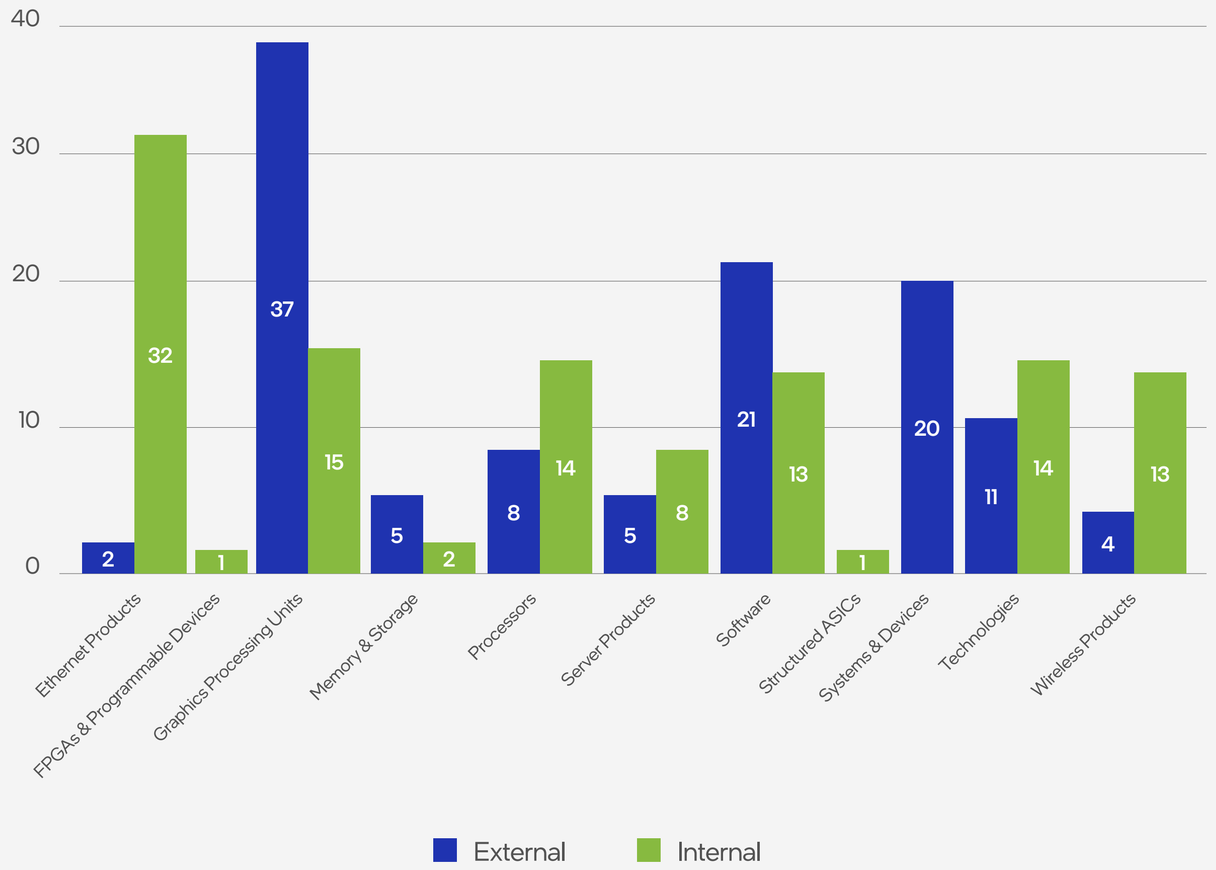
CVEs by Category - Internally/Externally Found

The scale of Intel's security capabilities is unmatched. To deliver security at scale, we have over 500 dedicated product security staff, perform over 120 hackathons per year, fund 40+ academic research teams, and continue to expand our Bug Bounty programs in innovative ways.

In 2021, 50% of the vulnerabilities addressed were found internally by Intel and 43% were reported through our Bug Bounty programs. The remaining 7% came from various sources such as open source projects managed by Intel and from organizations who do not or cannot seek bug bounty payments.

We continue to deliver on our Security First Pledge through investment, maturity of process, community engagement, and through transparency in reporting results.

2021 Product Categories by Internally/Externally Found



CVE Severity

2021 severity stats:

- 11% of vulnerabilities were rated low severity
- 65% of vulnerabilities were rated medium severity
- 23% of vulnerabilities were rated high severity
- 1% of vulnerabilities were rated critical severity.

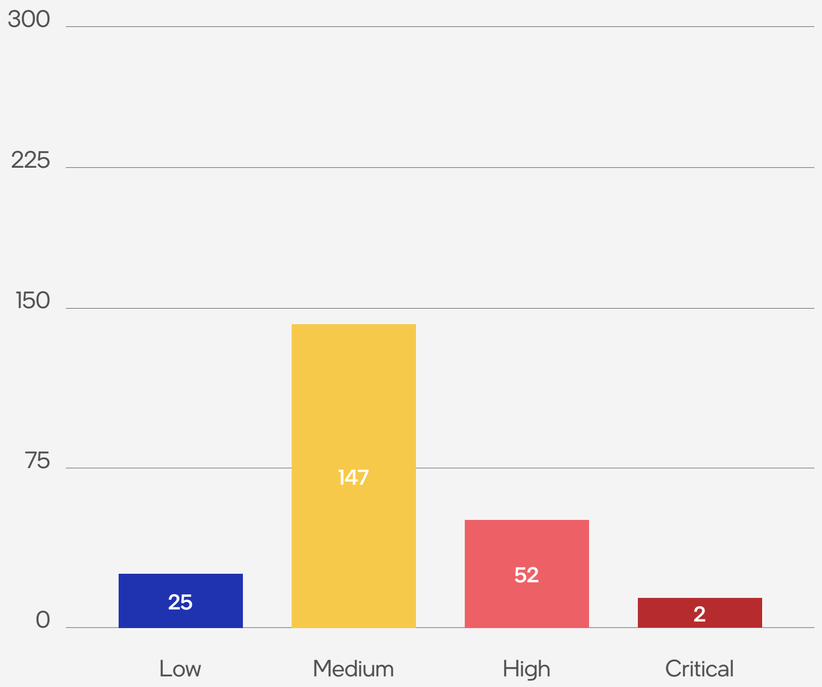
The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics.

The impact of most of the medium, high, and critical vulnerabilities is potential elevation of privilege. In the case of medium severity issues, these mostly require an authenticated user on the same physical network or who has physical or local access to a vulnerable system. These issues become high or critical if an unauthenticated user can trigger the vulnerability and/or they can reach a vulnerable system from outside of the local area network.

CVSS severity scores fall into five categories:

None:	0.0
Low:	0.1–3.9
Medium:	4.0–6.9
High:	7.0–8.9
Critical:	9.0–10.0

2021 Count of CVEs by Severity

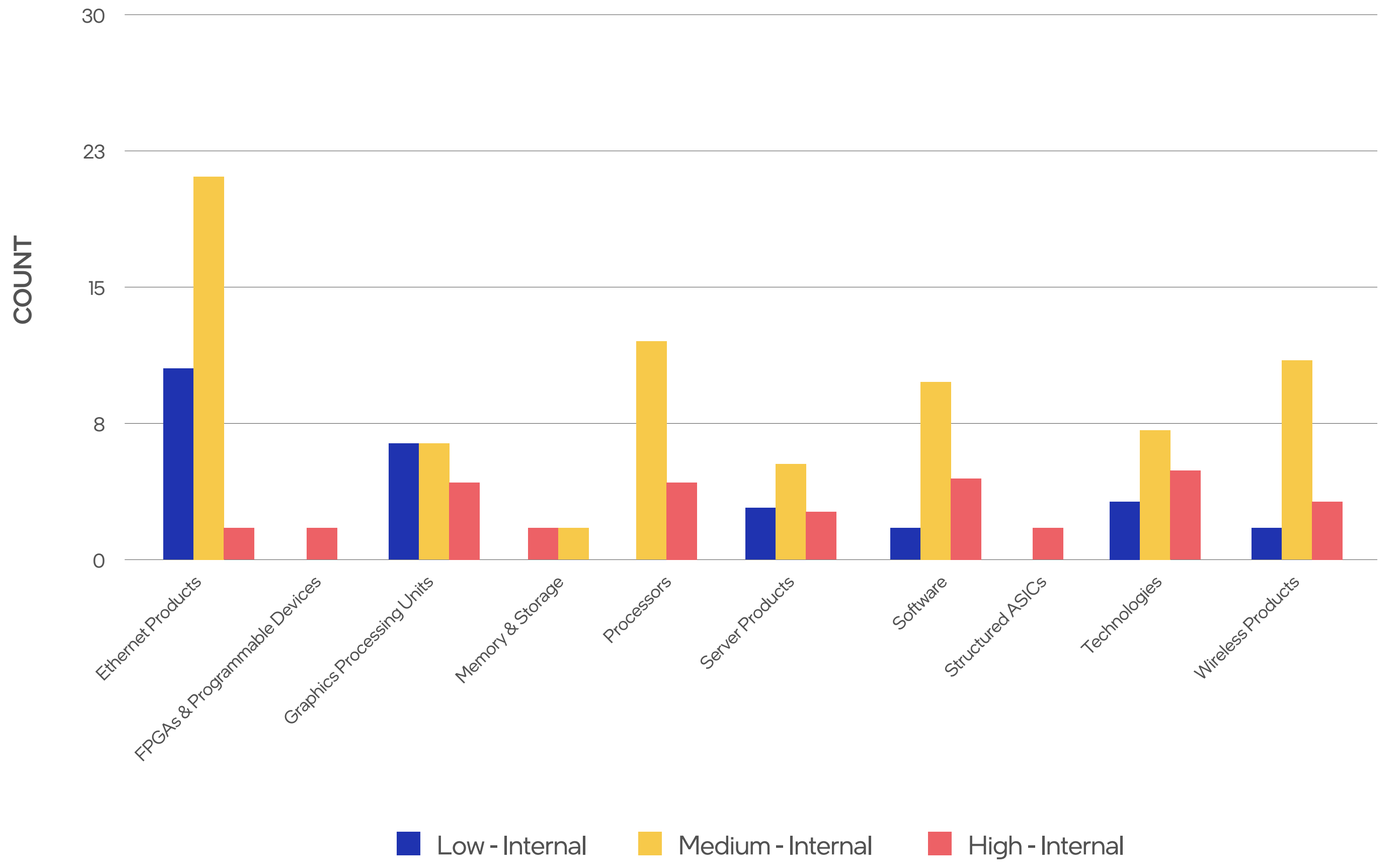


CVE DATA

Severity of Internally Found by Product Category

As part of Intel's commitment to transparency, these issues were assigned CVE ID's and publicly reported via an industry standard security advisory on https://intel.com/security.

Severity of Internally Found by Product Category



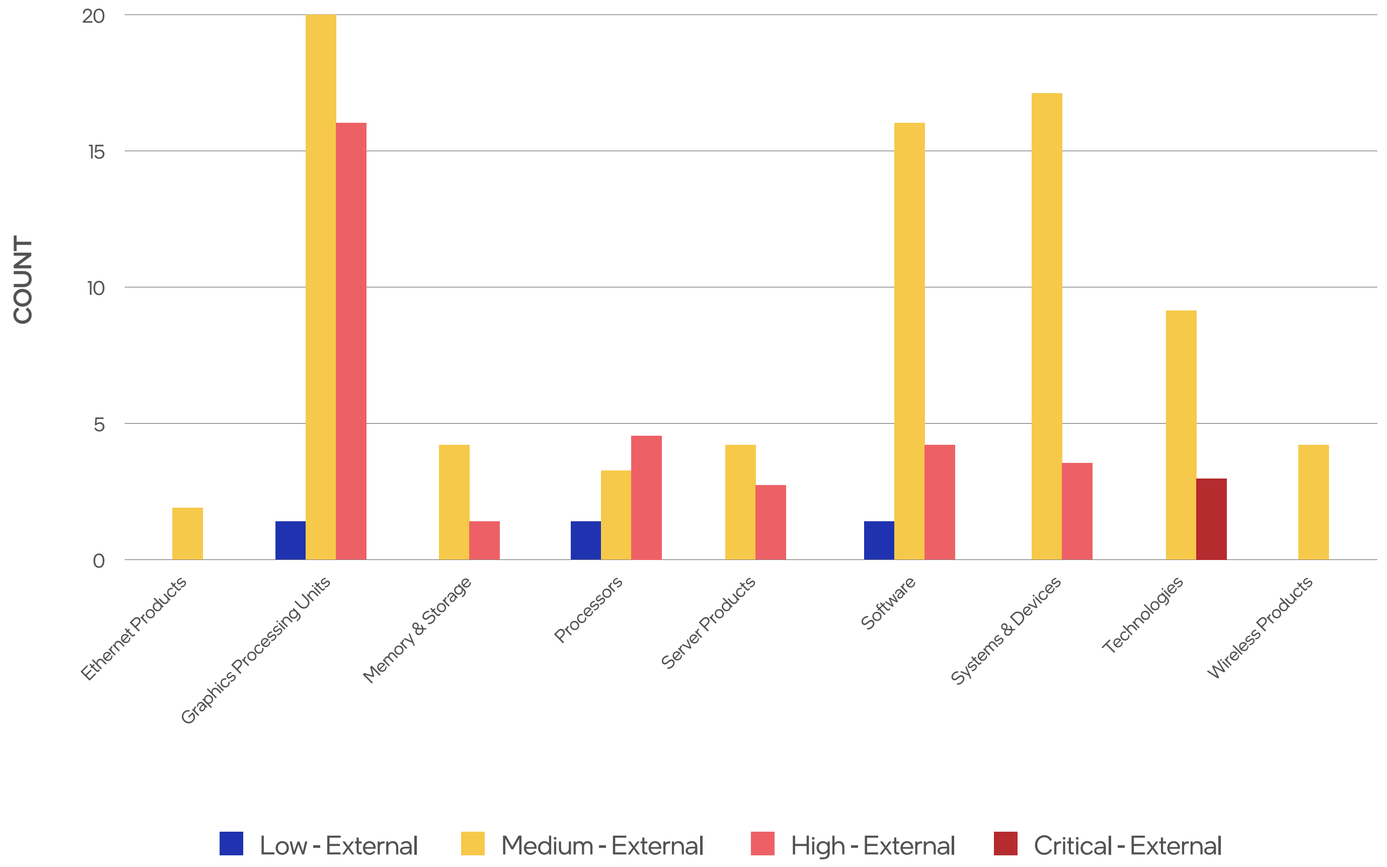
Severity of Externally Found by Product Category

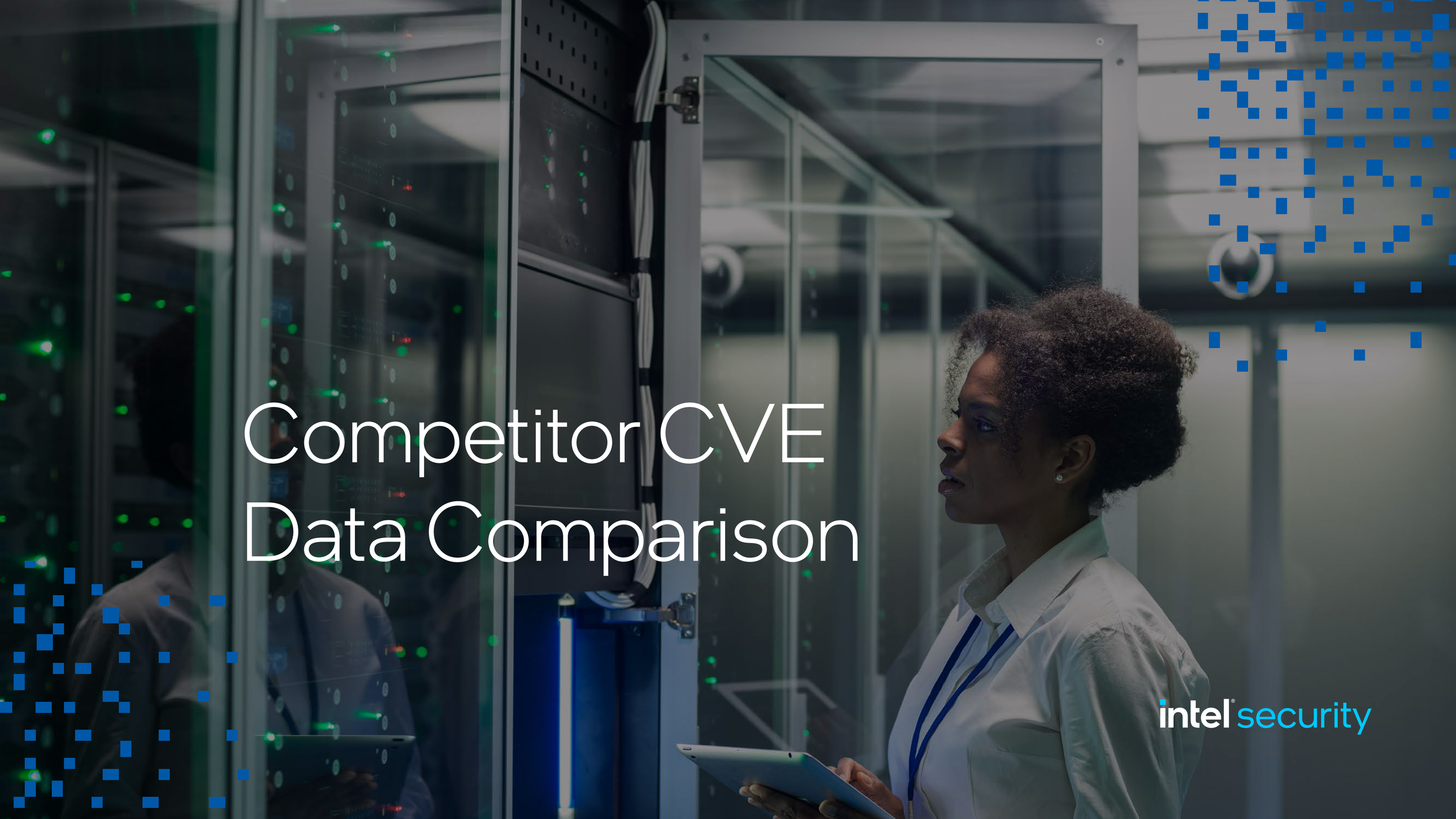
Of the 113 vulnerabilities reported by external researchers, 97 (86%) were reported through Intel's Bug Bounty Program.

The majority of external research in 2021 focused on software drivers for graphics, software products & utilities, and the System & Devices category covering Intel Server Boards and the Intel NUC products.

Note: 23 of the 37 vulnerabilities in the Graphics Processing Units category, were in third party components shipped as part of an Intel platform. See INTEL-SA-00481 for details.

Severity of Externally Found by Product Category





Competitor CVE Data Comparison

intel security

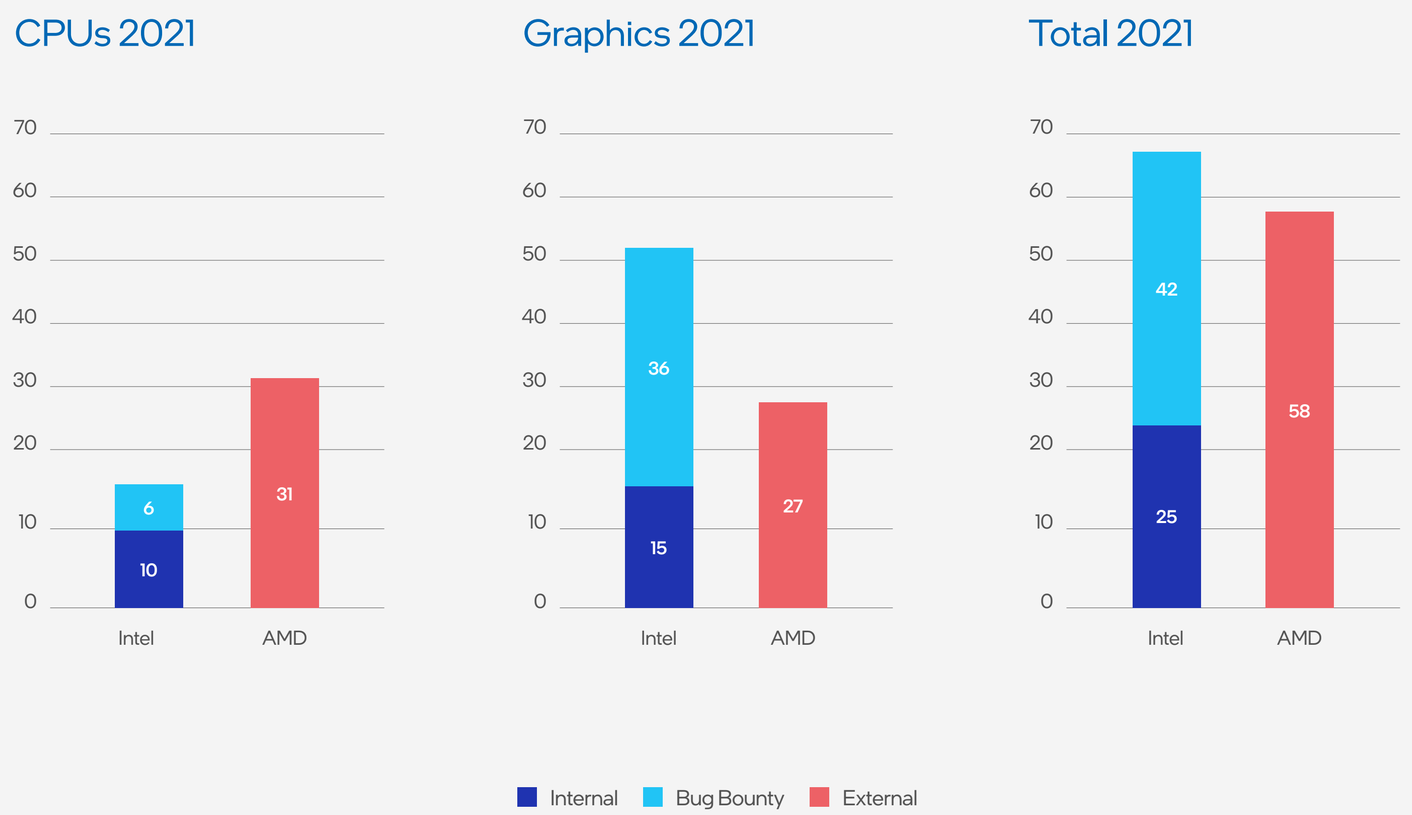
COMPETITOR CVE DATA COMPARISON

Intel & AMD CVE Data

Intel has a vast portfolio of products (as listed on intel.com) including many categories other silicon vendors do not compete in. In order to provide an accurate comparison, this report narrows CVE counts to two primary areas, CPUs and Graphics, and compares data with AMD, who also ships products in these categories.

In 2021, Intel reported 16 CPU and 51 graphics vulnerabilities (67 combined) while AMD reported 31 CPU and 27 graphics vulnerabilities (58 combined).

As previously noted in this report, our Security First Pledge guides us to transparently report vulnerabilities whether found internally or externally. We have not identified any AMD-published CVEs in 2021 attributed to AMD internal research. Therefore, the information in this comparison is based solely on AMD CVEs attributed to external research.



Note that AMD data is only available from May 2021 to December 2021.

COMPETITOR CVE DATA COMPARISON

CVE Data Sources

CVE data used in the comparison on the previous page was sourced from:

- Intel: intel.com/security
- AMD: amd.com/en/corporate/product-security

CPU data: CPUs, or processors, ship as platforms that often contain additional technologies such as Intel® SGX or the Intel® Converged Security and Management Engine (CSME) and efforts were made to capture this information from the data sources at right. For the purposes of this comparison, advisories for UEFI firmware updates are not included.

Graphics data: Graphics data was derived from advisories labeled as addressing graphics components. Note that INTEL-SA-00481 contains 23 CVE IDs affecting AMD components. 22 of the CVE IDs were assigned by AMD and included in AMD-SB-1000.

INTEL-SA-00438	Intel® Graphics Drivers Advisory
INTEL-SA-00444	Intel® SGX Platform Software Advisory
INTEL-SA-00455	Intel® SGX Platform Advisory
INTEL-SA-00459	2021.1 IPU – Intel® CSME, SPS and LMS Advisory
INTEL-SA-00464	2021.1 IPU – Intel® Processor Advisory
INTEL-SA-00465	2021.1 IPU - Intel Atom® Processor Advisory
INTEL-SA-00477	Intel® IPP and SGX Software Advisory
INTEL-SA-00481	Intel® Core™ Processors with Radeon™ RX Vega M GL Graphics Advisory
INTEL-SA-00500	Intel® SPS Advisory
INTEL-SA-00508	Intel® Graphics Drivers Advisory
INTEL-SA-00516	Intel® Processors Software Developer Guidance Advisory
INTEL-SA-00528	Intel® Processor Advisory
INTEL-SA-00566	Intel® Graphics Drivers Advisory

AMD-SB-1023	TLB Poisoning Attacks on AMD Secure Encrypted Virtualization (SEV)
AMD-SB-1021	AMD Server Vulnerabilities – November 2021
AMD-SB-1000	AMD Graphics Driver for Windows 10
AMD-SB-1017	Side-channels Related to the x86 PREFETCH Instruction
AMD-SB-1009	AMD Chipset Driver Information Disclosure Vulnerability
AMD-SB-1010	Transient Execution of Non-canonical Accesses
AMD-SB-1013	AMD Secure Encryption Virtualization (SEV) Information Disclosure
AMD-SB-1003	Speculative Code Store Bypass and Floating-Point Value Injection
AMD-SB-1004	AMD Secure Encrypted Virtualization

Resources

intel security

Podcasts & Videos

Podcasts

Links

[Intel 2019 Product Security Report]

[Intel 2020 Product Security Report]

[Intel Security Overview]

[Intel Security Technology Overview]

[Intel Product Security Center]

[Intel Security Newsroom]

Videos

Contributors

intel security

Intel thanks the following employees for their contributions to this report (listed in alphabetical order by last name):

Yavniella Angel

Momi Avital

Juliana Ball

Jerry Bryant

Amit Elazari Bar On

Jason Fung

Suzy Greenberg

Bat-sheva Honigstein

Shelby Ineson

Matthew Johnson

Camille Morhardt

Ron Moussafi

Yanai Moyal

Yair Netzer

Kathleen Noble

Christopher (CRob) Robinson

Shai Sarfaty

Itamar Sharoni


intel
security

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.

Reference

intel security

REFERENCE

Intel Product Categories

Intel product and product sub-categories can be found at www.intel.com, then click on “Products” from the menu.