2020 Product Security Report

intel security

Security doesn't just happen. It's the result of unwavering focus that guides everything we do to research, architect, build, and support products customers can trust.

intel security


2020 Key
Findings
intel security

92% of vulnerabilities addressed are the direct result of Intel's investment in product security assurance

47% 109 of the 231 CVEs (47%) published were discovered internally by Intel employees

45% 105 of the 231 CVEs (45%) were reported through Intel's Bug Bounty Program

69% of firmware vulnerabilities were found by Intel while 83% of software issues (device drivers and software utilities) were found by external researchers

0 None of the 231 vulnerabilities addressed in 2020 are known to have been used in actual attacks

Foreword

If 2020 showed us anything, it is the continued need for vigilance in keeping systems up to date with the latest mitigations.

The realized threat of supply chain attacks requires organizations to understand not only what third-party products they are using, but also the disposition of those products from an attack surface perspective. This requires transparency in the supply chain.

Transparency is part of Intel's security first commitment and this report is representative of how we seek to lead through accountability. In an ever-changing threat landscape, providing the right information for customers to properly assess risk is a responsibility we embrace as we continue on our journey to be the trusted performance leader that unleashes the potential of data.

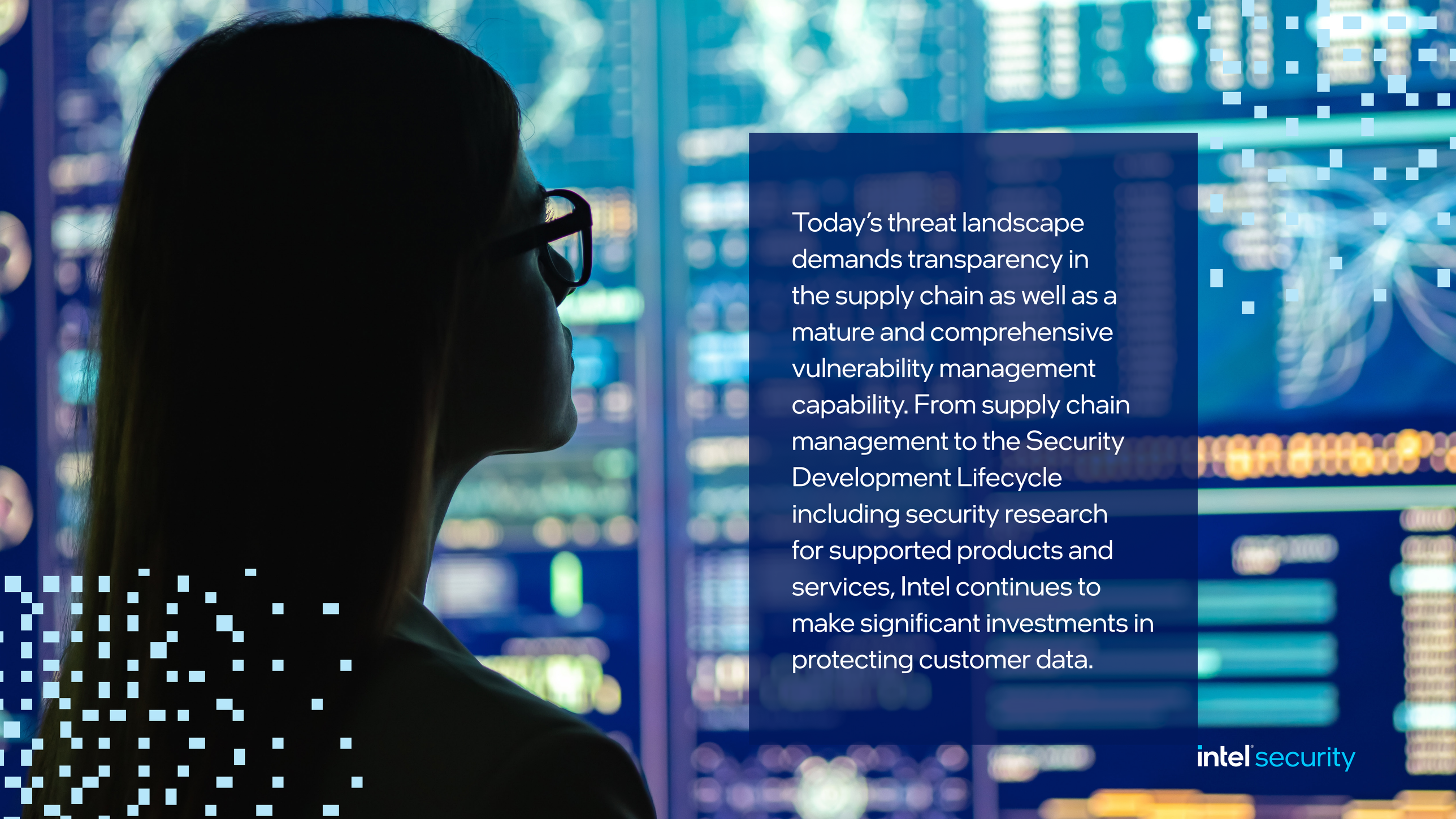
We design with security in mind. Developing the strongest products demands that security is more than a one-time event. It's a shared responsibility that prioritizes power and performance as well as security. Our approach is driven by extensive research and continuous integration of what we learn throughout our development processes and practices. All designed to deliver security assurance as we advance the state of the art in our products.

The 2020 Intel Product Security Report demonstrates our continued focus and investment in building the most trusted platform in the world, proactively seeking to find and mitigate security issues, and protecting customers through the transparent and timely delivery of mitigations.

In 2020 we delivered mitigations for 231 product security issues. 109 (47%) were internally found by Intel employees through our efforts around offensive security research and another 105 (45%) were reported through Intel's Bug Bounty program. In total, 92% (214) of the issues addressed were the direct result of our ongoing investment. The remaining 17 issues were reported to Intel by partners or organizations who do not typically seek bounty payments.

While our internal focus tends to lean towards core platform protection, such as the Intel® Converged Security and Management Engine (Intel® CSME) and related firmware updates, the bulk of external research continues to yield results in software drivers (graphics and networking components) and within the vast array of software utilities available in the Intel download center.

"We design with security in mind."



Today's threat landscape demands transparency in the supply chain as well as a mature and comprehensive vulnerability management capability. From supply chain management to the Security Development Lifecycle including security research for supported products and services, Intel continues to make significant investments in protecting customer data.

intel security


Investing
in Security
Assurance
intel security

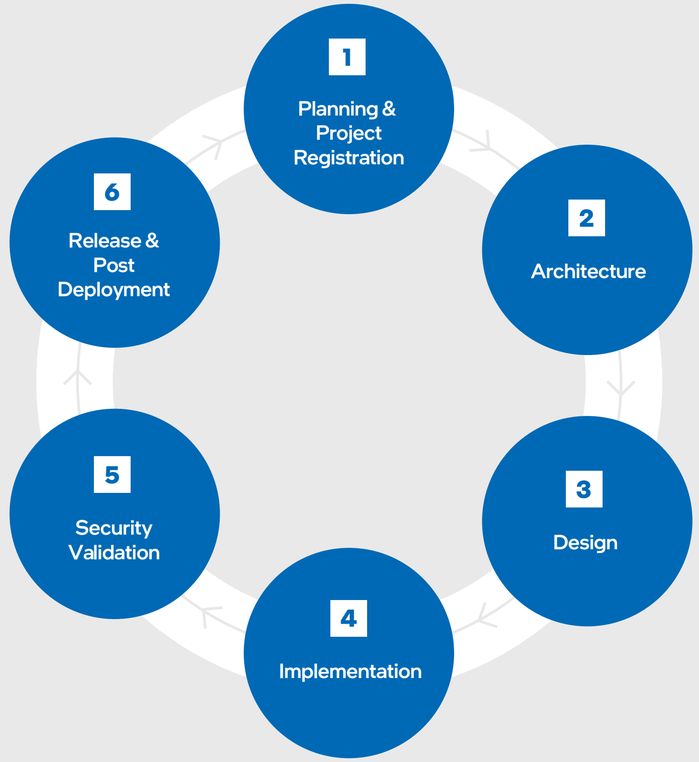
Security Development Lifecycle (SDL)

Developing products with a security mindset is an important industry practice that reduces mitigation costs and improves product resiliency.

The SDL is a set of processes that implement security principles and privacy tenets into product development. These processes incorporate security minded engineering and testing at the onset of product development when it is more effective and efficient to employ. SDL is part of Intel's comprehensive product security assurance approach. Other aspects of Intel's approach include training, conferences, the Product Security Incident Response Team (PSIRT), the Bug Bounty program, research (offensive and defensive), and industry collaborations.

While SDL is most common in software development, Intel has been applying these principles across software, firmware and hardware development since at least 2009. Intel's Security and Product Assurance organization was formed in 2018, furthering the implementation of security best practices like SDL. The methodology and adoption of SDL continue to evolve.

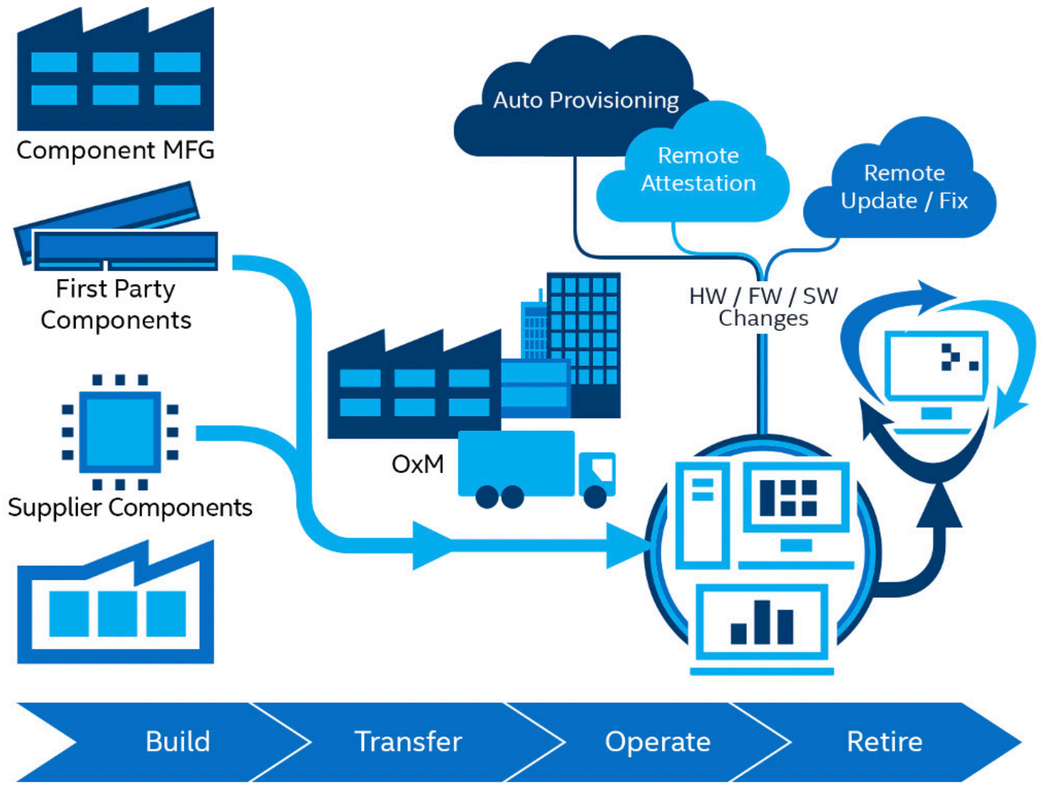
1. **Planning and Assessment.** Determine security and privacy risks and identify tasks and activities necessary to address them.
2. **Architecture.** Define security objectives and use them to build an appropriate threat model.
3. **Design.** Perform security and privacy analysis based on security objectives, threats, and requirements identified in previous phases.
4. **Implementation.** Perform secure code reviews and static code analysis, and check that architecture and design are performing as intended.
5. **Security Validation.** Employ vulnerability scanning, fuzzing, penetration testing and other methods to ensure product requirements have been met and make "ship / no ship" determination.
6. **Release and Post Deployment.** Conduct testing to ensure previously detected issues have been resolved and continue to scan for vulnerabilities in third-party components and IP. Implement plan to monitor and manage security for the lifespan of the product.



For more information on Intel's SDL program and how it fits within our security initiatives, visit **newsroom.intel.com/press-kits/intel-security-initiatives.**

Compute Lifecycle Assurance (CLA)

Addressing platform integrity throughout the lifecycle of service.



Compute Lifecycle Assurance was developed with key initiatives for preventing, resolving, innovating and leading in the security industry. Intel's holistic security action plan includes:

- Establishing an end-to-end framework (CLA) that can be applied across the multi-year life of any platform to substantially improve transparency and to provide higher levels of assurance.
- By enabling transparency and assurance across a system's lifecycle, supply chain owners can improve platform integrity, resilience and security.
- Building assurance through each stage of the lifecycle (build, transfer, operate, and retire).
- Creating a community to address supply chain assurance and transparency.

Offensive Security Research

To help guide Intel security development investments and focus areas, we employ a robust Offensive Security Research program as part of our mission to deliver on our security goals.

Our efforts are led by dedicated teams of security researchers who role model industry-leading practices with specific focus in three areas:

Proactive Research

Intel researchers continually monitor and probe Intel products and platforms for known and emerging threats and attacks; conduct in-depth adversarial analysis of technology architecture; continually evolve threat models; identify new vulnerabilities and exploits; and develop systemic mitigations to resolve the vulnerabilities and weaknesses. Examples:

- **Architecture Review:** Assess against Security Objectives
- **Vulnerability & Exploitation:** Find novel vulnerabilities & develop Proof of Concept exploits
- **Systemic Mitigations:** Eliminate classes of vulnerabilities

Reactive Research

These efforts are driven by swift threat landscape and intelligence detection of newly discovered vulnerabilities and exploits that require systemic mitigation strategies. Examples:

- **Triage of incoming vulnerability reports:** Verify findings and assess risks
- **Mitigation effectiveness of identified vulnerabilities:** Vet mitigations addressing root cause

Capabilities and Culture

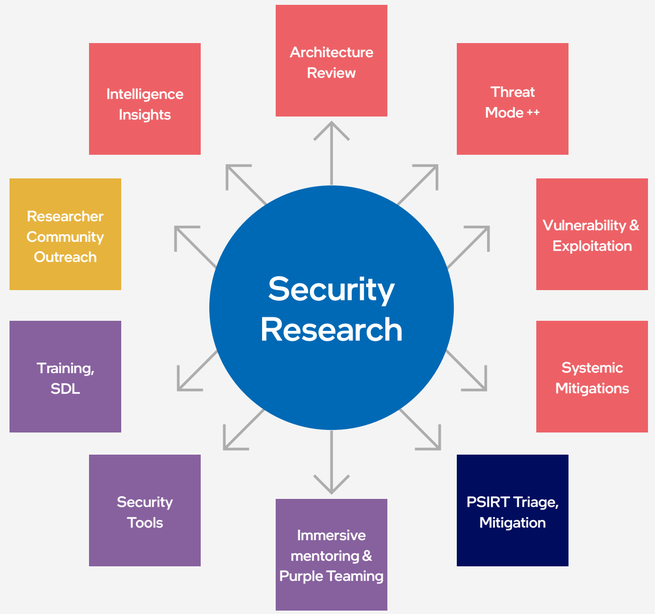
Solutions focused on driving the security-first mindset and getting every Intel architect, developer, designer, and validator to instinctively think like a hacker would, embracing learnings. Examples:

- **Immersive mentoring:** A company-wide Red Team Community
- **Purple Teaming:** Security Hackathons for Blue & Red teams together
- **Security Tools:** Research, prototype, and deploy breakthrough tools
- **Training:** Generate new content from research to train Intel engineers
- **SDL improvements:** Develop new guidance for SDL

Researcher Community Outreach

Substantial investments to engage the global security research community across the industry and the academia. Examples:

- **Listening events:** Understand industry security researcher perspective
- **Research sponsorship:** Sponsor universities conducting novel research



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 75 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 contributes to the Common Vulnerability Scoring System (CVSS) and helps lead the Product Security and Incidence Response (PSIRT) special interest group where Intel employees co-authored the PSIRT Services Framework as a contribution to the global security community.

Bug Bounty Program

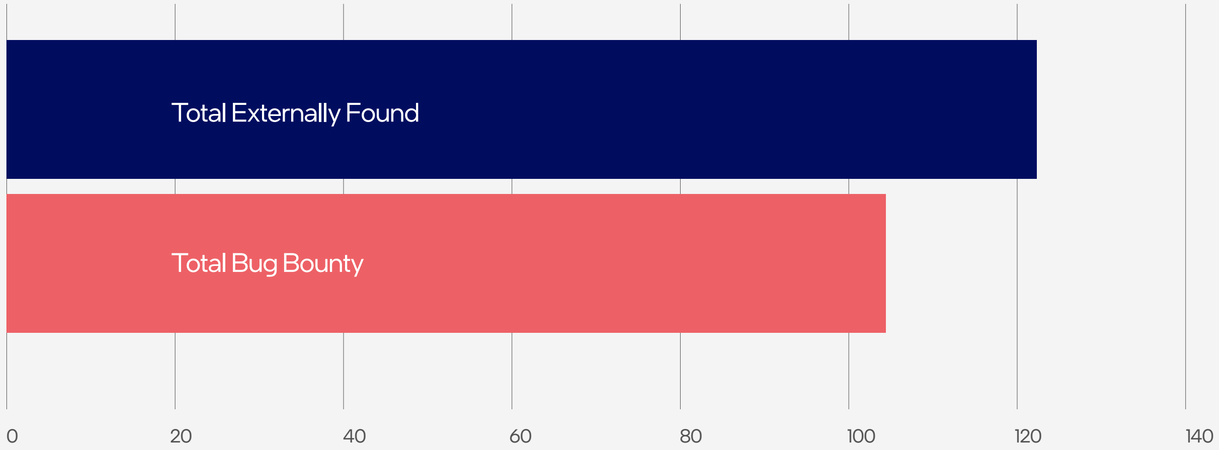
Intel believes that working with skilled security researchers across the globe is a crucial part of identifying and mitigating security vulnerabilities.

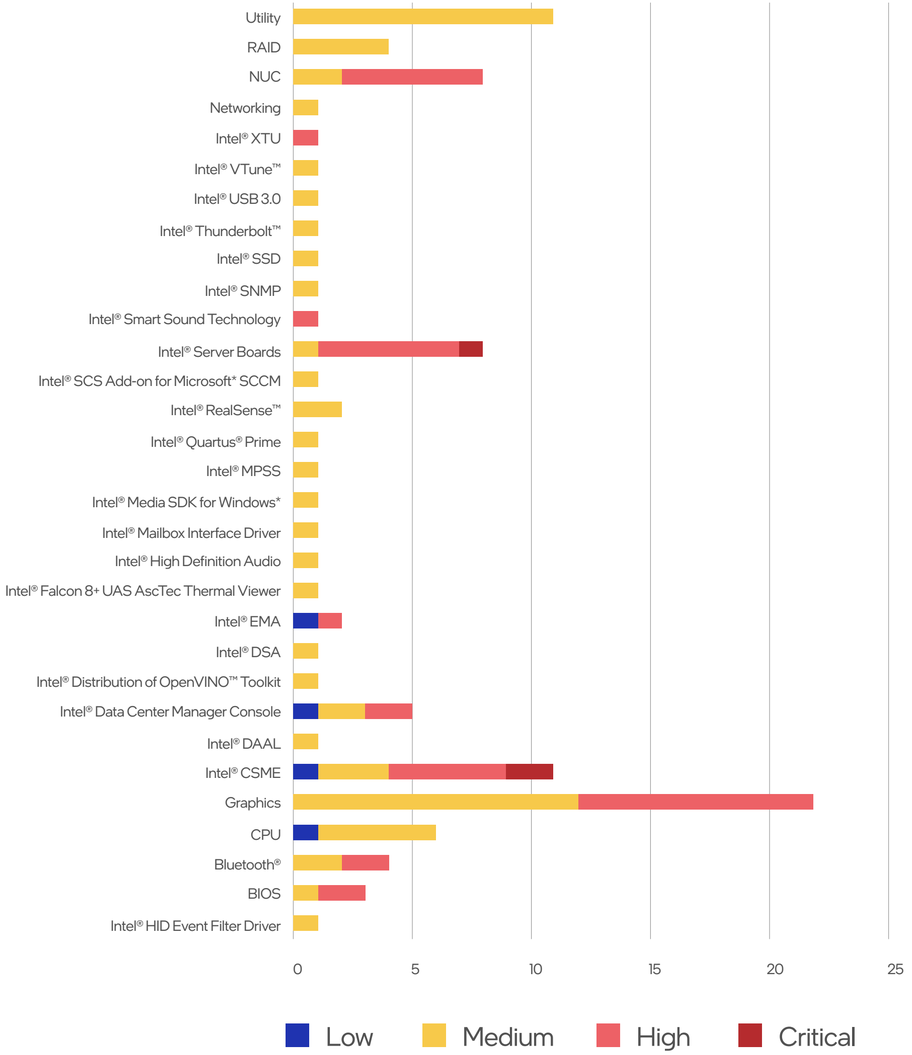
To incentivize researchers to focus on Intel products, we established the bug bounty program in 2018 and have paid out an average of $800,000.00 per year.

In 2020, there was a 33% increase in bounty submissions resulting in a published CVE ID count of 105 compared to 70 in 2019. At the same time, we saw a 62% increase in the number of unique external security researchers we engaged with.

Intel's Bug Bounty program resulted in the coordinated public disclosure of 45% (105) of the vulnerabilities addressed in 2020.

86% of External Reports are from the Bug Bounty



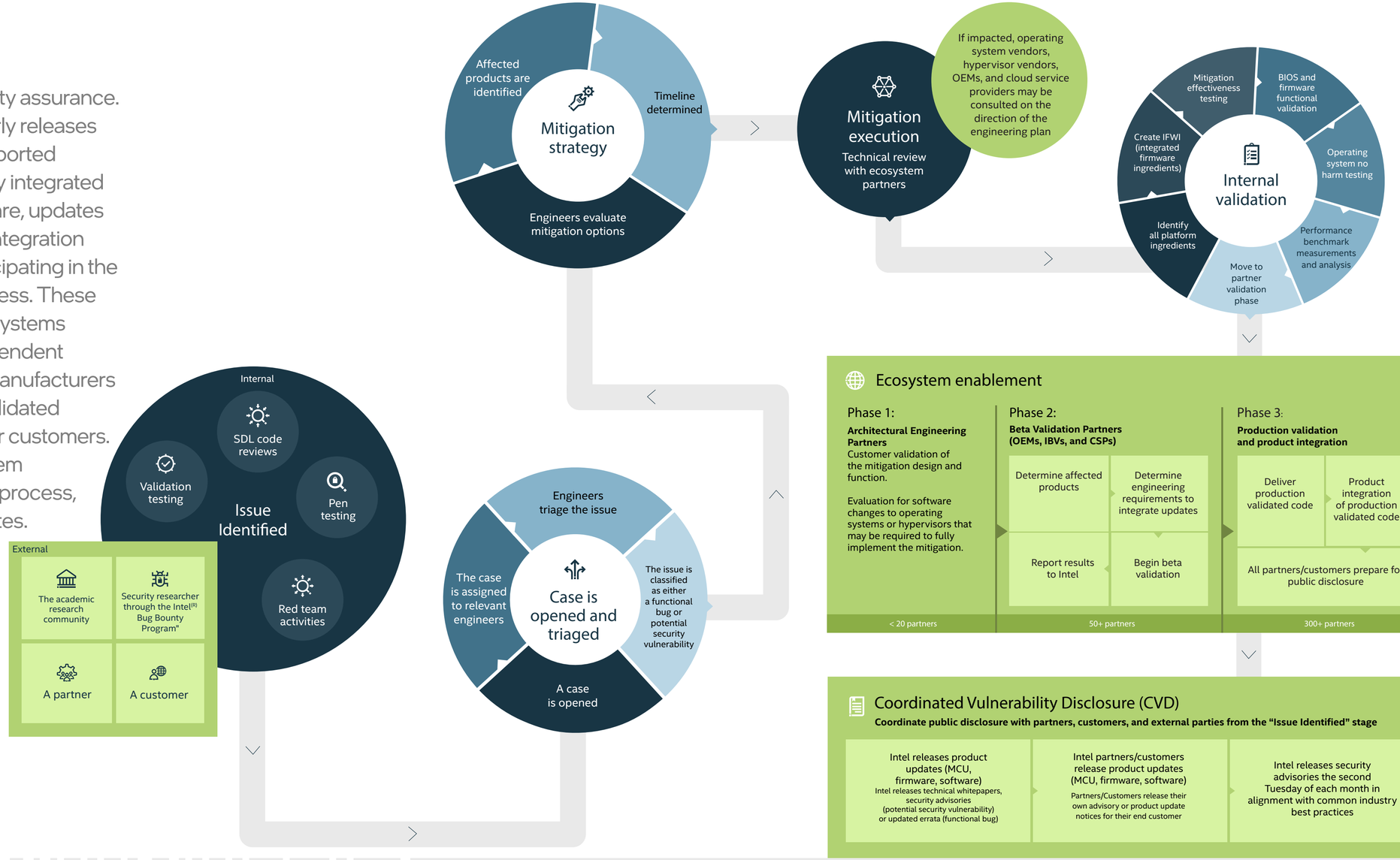


More information about Intel's bug bounty program can be found at **intel.com/security.**

Intel Platform Update (IPU)

Intel is committed to product and security assurance.

Intel is committed to product and security assurance. As part of this commitment, Intel regularly releases functional and security updates for supported products and services. Due to the highly integrated nature of hardware, firmware and software, updates often require additional validation and integration from Intel's ecosystem of partners participating in the coordinated vulnerability handling process. These ecosystem partners include operating systems vendors, cloud service providers, independent firmware vendors, original equipment manufacturers and systems integrators who release validated updates through direct channels to their customers. The IPU process facilitates the ecosystem coordination and vulnerability handling process, leading to the release of validated updates.



Results of Intel's Investments in Security Assurance

The identification and mitigation of product security issues is a critical focus area for Intel.

Our efforts continue to yield positive results allowing our customers to rely on our capability to discover and coordinate these issues through a timely public disclosure.

Intel's continued investments in product security assurance resulted in 92% of the CVEs addressed in 2020.

Internal security research, including SDL related scanning, fuzzing, pen testing, and red team events, accounts for 47% of the vulnerabilities addressed.

An additional 45% of vulnerabilities were reported through Intel's bug bounty program.

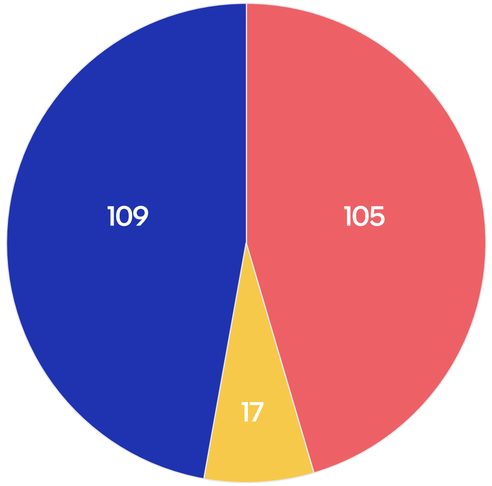
In 2020, we addressed 231 vulnerabilities compared to 236 in 2019. The 2020 data shows a more even split between internally found issues and those reported through the bug bounty program.

Issues in the "other" bucket include vulnerabilities reported by Intel partners, customers, and those reported by organizations who do not or cannot seek bounty payments.

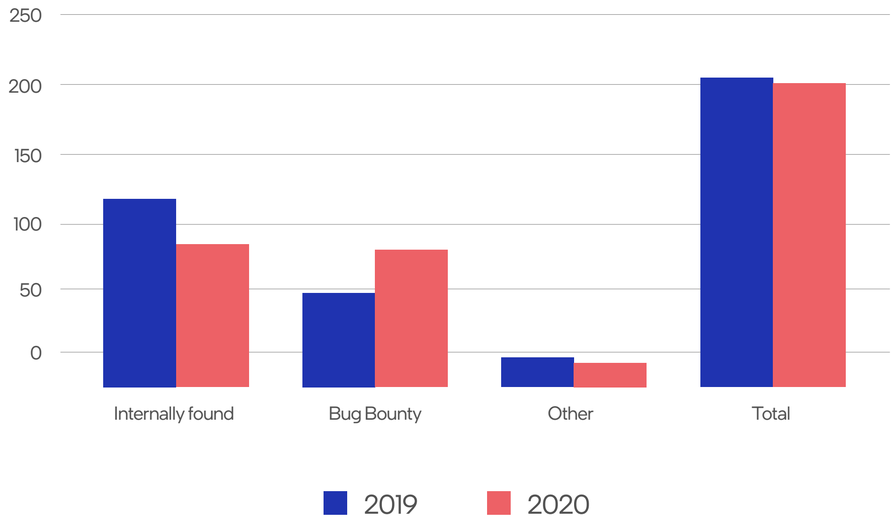
2020 Overview

In 2020, 92% of vulnerabilities addressed were the result of Intel's ongoing investments in security research.

- Internally Found
- Bug Bounty
- Other



2019 Comparision



CVE Data

By category and severity

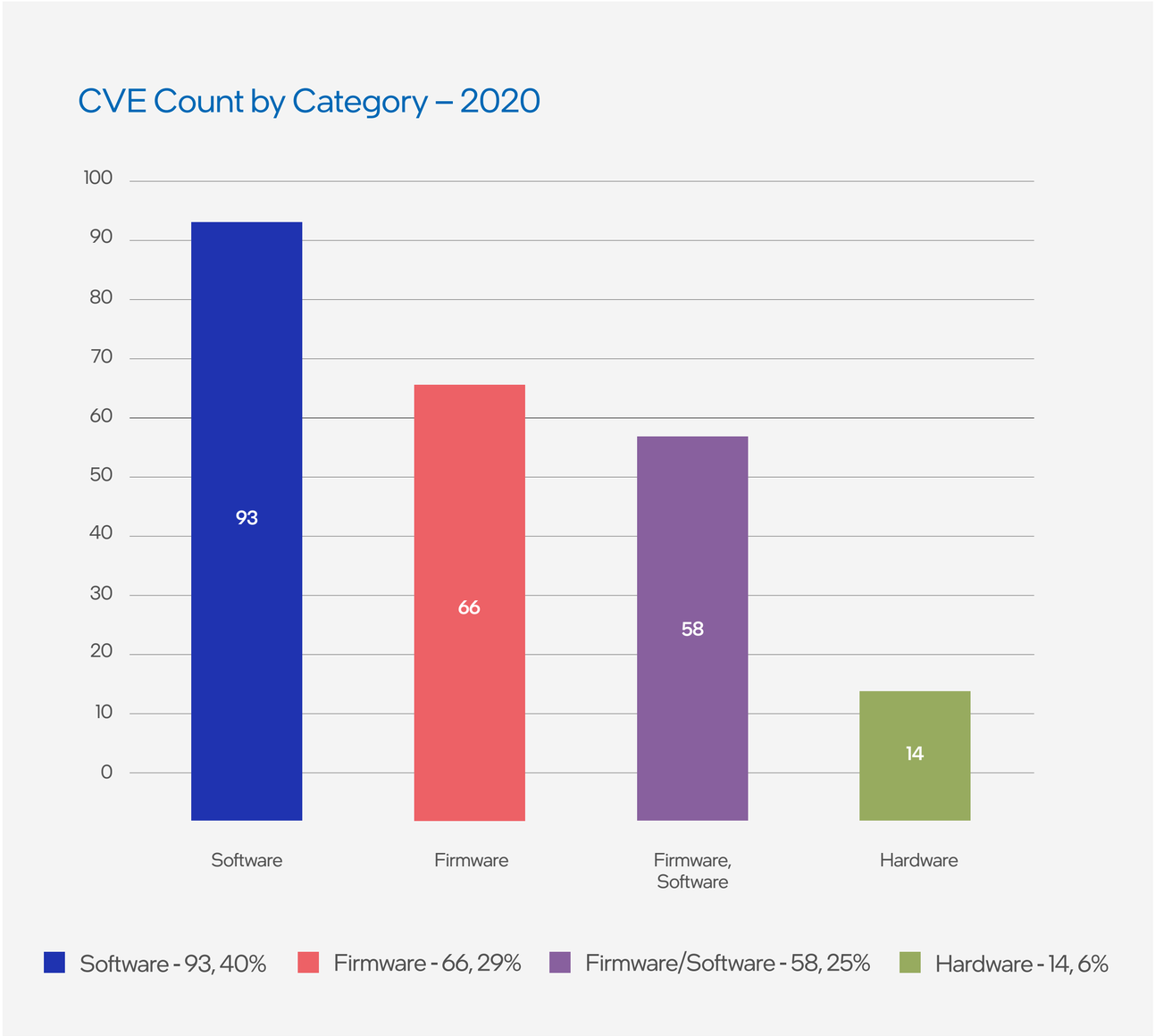
intel security

CVE Data

CVEs by Category

Intel Security Advisories are divided into three primary categories: software, firmware, and hardware.

In some cases, a complete mitigation may require a software driver update and a firmware update, so this combination is called out separately.



CVEs by Category

As this report will demonstrate, the bulk of externally found issues were in software consisting mainly of software utilities and software drivers for graphics, networking, and Bluetooth ™ components.

While these are important issues to address, our product firmware forms the basis of trust in our platforms and the data shows this is the primary focus of our internal security research. When combining the firmware and the firmware + software categories, 69% of vulnerabilities addressed were found by Intel as were 57% of hardware issues.

Further breakdown of categories:

Software includes:

- Software only driver updates
- Applications
- Utilities

Firmware includes:

- Intel®Management Engine
- BIOS/UEFI
- Authenticated Code Module (ACM)
- Networking product firmware
- Graphics firmware

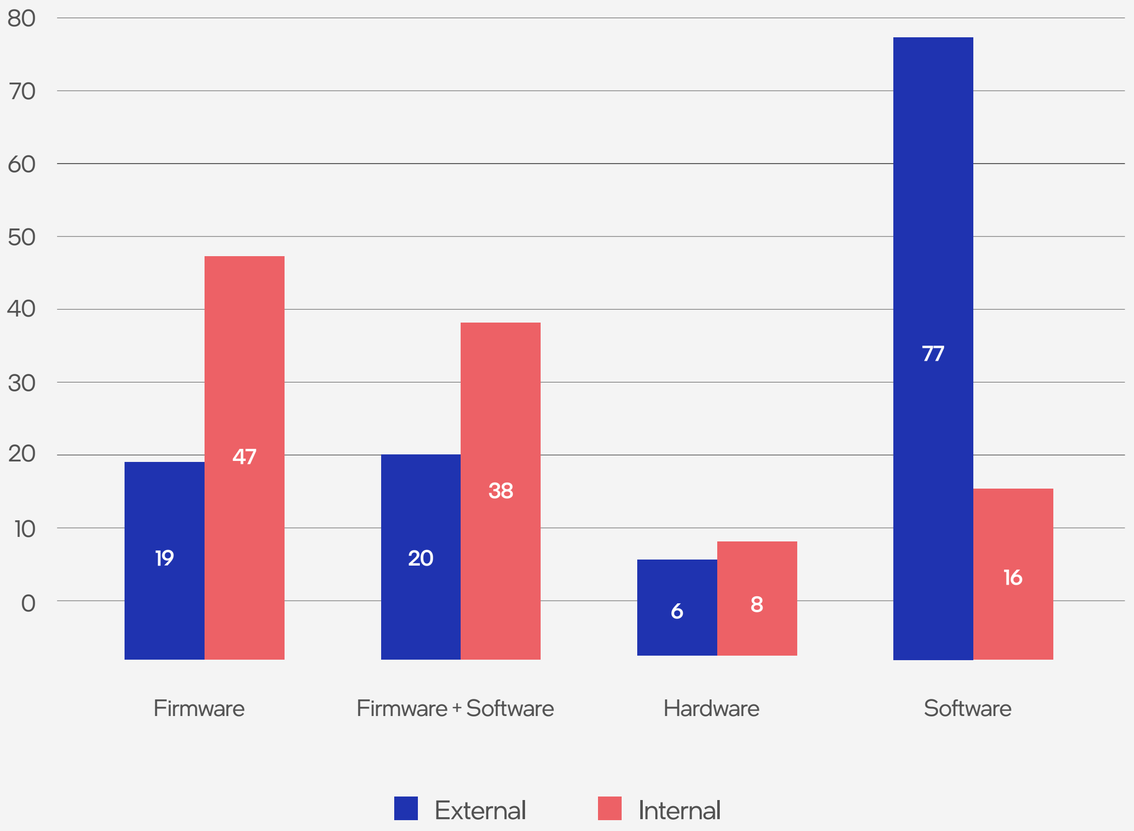
Firmware and Software includes:

- Instances where the above software and firmware updates are delivered together to mitigate an issue.

Hardware includes:

- Microcode updates

2020 Categories by Internally/Externally Found



CVE Severity

2020 severity stats:

- 6% of vulnerabilities were rated low severity (64% found by Intel).
- 57% of vulnerabilities were rated medium severity (43% found by Intel).
- 35% of vulnerabilities were rated high severity (51% found by Intel).
- 3% of vulnerabilities were rated critical severity (33% found by Intel).

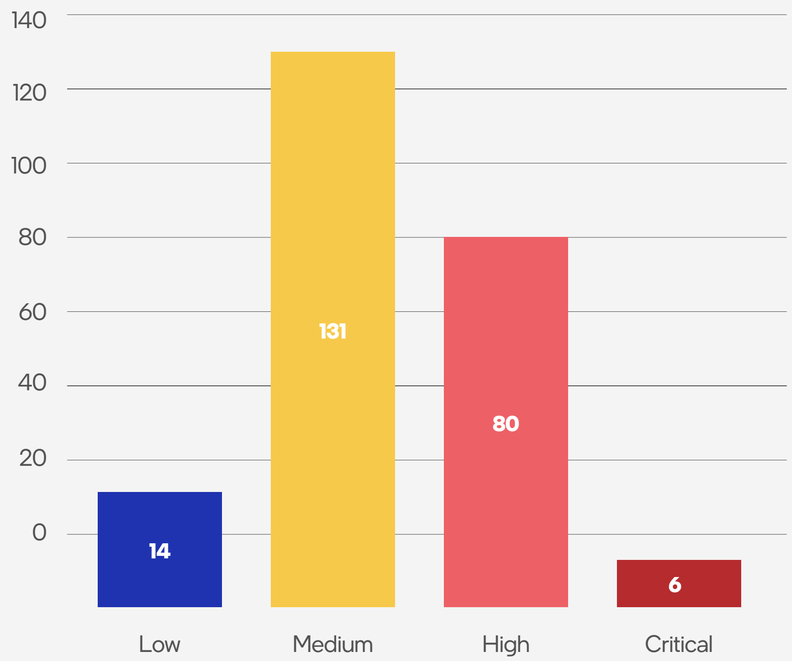
The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant 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 require an authenticated user on the same physical network or who has physical 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 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

2020 Count of CVEs by Severity

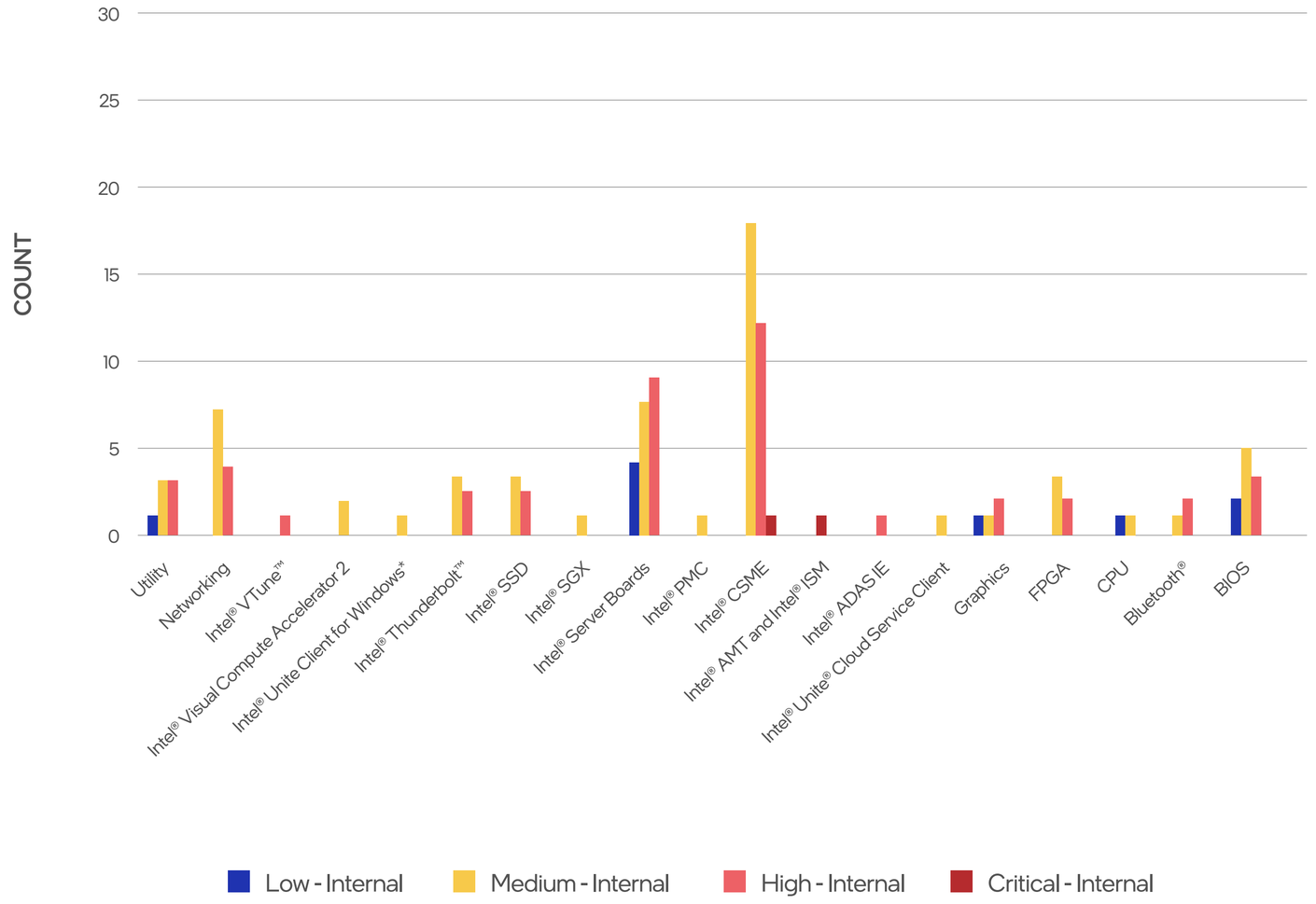


CVE Data

Severity of Internally Found by Product Area

The majority of High and Critical severity issues were found internally by Intel.

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 intel.com/security.



For more information about Intel security advisories, visit **intel.com/security**.

CVE Data

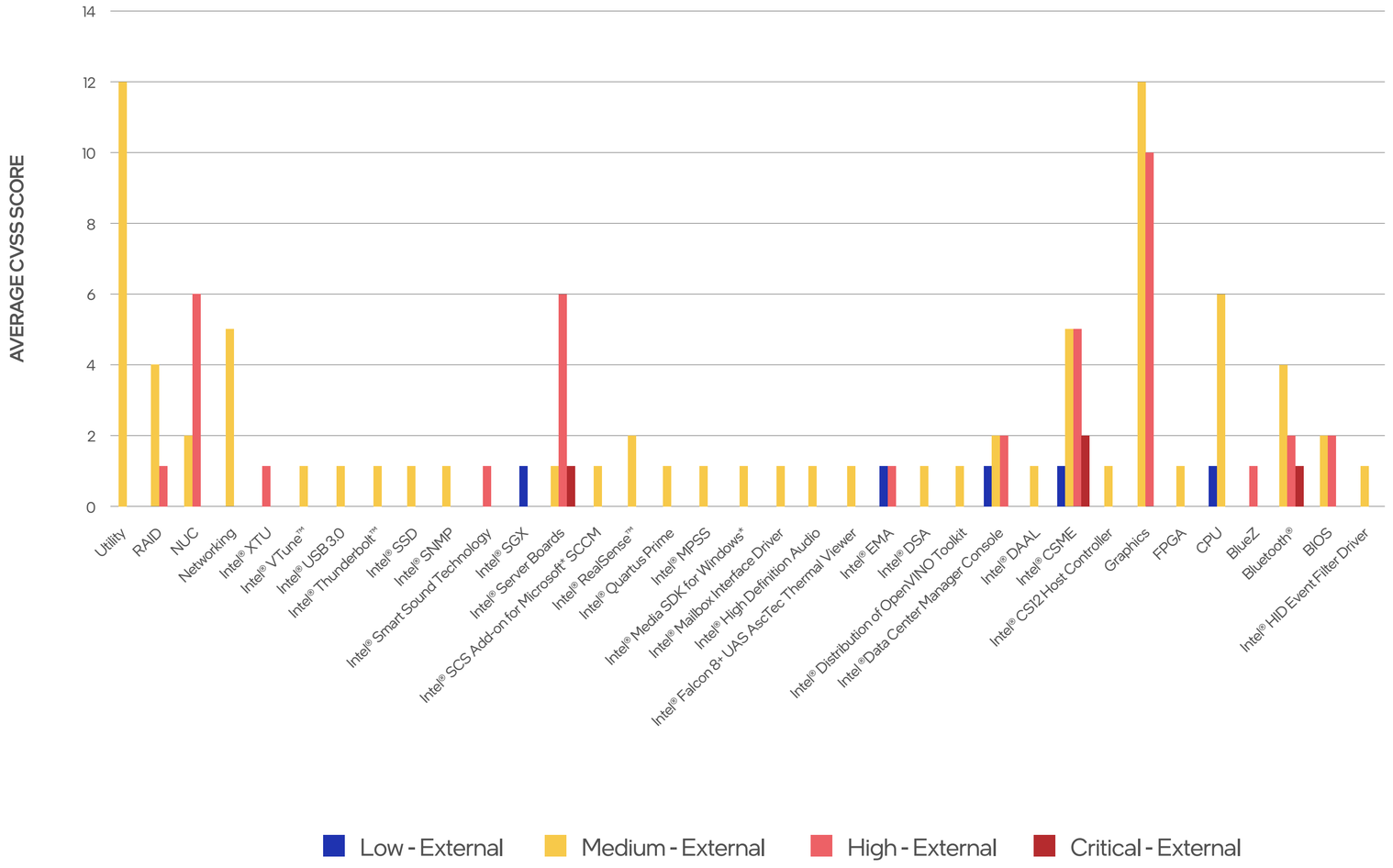
Severity of Externally Found by Product Area

Of the 122 vulnerabilities reported by external researchers, 105 (86%) were reported through Intel's Bug Bounty Program.

The majority of external research in 2020 focused on software drivers for networking, graphics, and Bluetooth® components followed by potential vulnerabilities in various software utilities available for download in the Intel download center.

We continue to see great firmware level research as well resulting in mitigations for Intel® CSME and Intel® Server Boards among others.

The CPU column addresses potential side-channel vulnerabilities based on research from academic institutions and organizations focusing heavily on security research.



For information about Intel vulnerability handling guidelines, visit **intel.com/content/www/us/en/security-center/vulnerability-handling-guidelines.html**.

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation.

Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.


intel
security